

# A LAS VEGAS REWRITING ALGORITHM FOR THE SYMMETRIC SQUARE REPRESENTATION OF CLASSICAL GROUPS

BRIAN P. CORR

*Dedicated to the memory of Ákos Seress, who provided a great deal of input into this work.*

ABSTRACT. In constructive recognition of a representation of a Classical group  $G$ , much attention has been paid to the natural representation as well as to generic (Black Box) algorithms that treat all representations uniformly. There are theoretical and practical improvements to be made by giving special treatment to certain non-natural representations that arise frequently. In this paper we present and analyse a Las Vegas algorithm for rewriting the Symmetric Square representation.

## 1. INTRODUCTION

A major goal of Computational Group Theory is the solving of the *constructive recognition problem*, which asks for fast (that is, polynomial time where possible) algorithms for the following tasks:

- (i) Given a group  $G < H$  input into a computer in some arbitrary way, determine the isomorphism type of  $G$  (*nonconstructive recognition*); and
- (ii) Produce an isomorphism from  $G$  into some ‘standard copy’ of this type of group, and provide a scheme for, given  $g$  in the ‘ambient’ group  $H$ , deciding if  $g \in G$ , and if so, rewriting  $g$  in this ‘standard form’ (*constructive recognition*).

The most common ways of inputting a group into a computer are as a set of generators and relations, or as a set of generating permutations or matrices: much effort has been spent in dealing with each of these representations separately, as well as in dealing with *Black Box Groups*, a theoretical setting in which no structural information about the way in which the group is represented is assumed.

Black Box algorithms provide complete generality, and hence apply in all settings: in particular, if the representation of  $G$  in the computer does not offer much information, then a Black Box algorithm will approach ‘maximal effectiveness’. On the other hand, particularly natural representations of a group (for example, the representation of the Symmetric Group  $S_n$  as permutations of  $n$  points, or the natural representation of the General Linear Group) can be dealt with much more quickly and effectively using methods specific to the representation.

---

This research forms part of the ARC Discovery Project DP110101153. The author was supported by an Australian Postgraduate Award, a UWA Top-Up Scholarship, an Australian Mathematical Society Lift-Off Fellowship and by cNPQ and CAPES. The author wishes to thank Cheryl Praeger and Ákos Seress for their support and input.

The ‘Composition Tree’ framework [11, 17] provides an elegant method for dealing with arbitrary matrix groups: using various methods, beginning with the MEAT-AXE procedure of Holt & Rees [7], the input group  $G$  is searched for normal subgroups  $N$ , and a structure is set up so that  $N$  and  $G/N$  may be dealt with separately. This process, applied recursively, yields a binary rooted tree that gives the procedure its name.

As with many group-theoretic frameworks relying on normal subgroups, the process terminates when  $G$  is almost simple (at the leaves of the tree). Each almost simple group presents its own unique challenges, and each family of almost simple groups is dealt with separately. In the matrix group setting, the Classical groups have received a great deal of attention, beginning with the Neumann-Praeger non-constructive SL-recognition algorithm [16]: the problem has essentially been solved in the Black Box cases (which make no attempt to exploit the geometry of the situation) and in the natural representation (where the geometry is most rich): see [20] for a survey. Attention is now paid to the remaining representations for which there is still meaningful geometric information to use.

In this paper we provide an updated and corrected version of the Magaard-O’Brien-Seress algorithm for constructively recognising the Special Linear Group in its action on the Symmetric Square module, and apply similar methods to constructively recognise all Classical groups (Unitary, Symplectic and Orthogonal) in their actions on the unique irreducible  $FG$ -module of dimension  $n$ , where  $\binom{d+1}{2} - 2 \leq n \leq \binom{d+1}{2}$  (in practice, this procedure will work perfectly well when the module is, in fact, the Symmetric Square, though in some cases the Symmetric Square is reducible). We wish to acknowledge and thank Cheryl Praeger and Ákos Seress for their support, expertise and advice during the preparation of this paper.

**Theorem 1.1.** *Let  $X \subseteq \text{GL}(n, q)$  be a set of matrices generating a classical group  $G = \text{Class}(d, q)$ , such that the module  $W$  defined by the action of  $H = \langle X \rangle$  is an irreducible section of the Symmetric Square module  $S^2(V)$  of codimension at most 2. Let  $d'$  be as in Table 2, and suppose that  $G \notin \{\text{Sp}(d, 3), \text{SO}^\epsilon(d, 3)\}$ . Then assuming that Conjecture 7.13 holds in the Symmetric Square case, and excluding some small values of  $d$  (see Table 1), there exists a Las Vegas algorithm which, with probability at least  $1 - \epsilon$ , sets up a data structure for rewriting  $H$  as a projective representation in its natural dimension, with complexity*

$O(\xi_H d^2 \log^2 q \log \epsilon^{-1} + \rho_q (d^9 \log d \log \log d \log q + d^8 \log d \log \log d \log^3 q \log \epsilon^{-1}))$ , where  $\xi_H$  is the cost of choosing a random element of  $H$ , and  $\rho_q$  is the cost of a field operation in  $\mathbb{F}_q$ . Once the initialisation procedure is complete, there is a Las Vegas algorithm for rewriting a group element (that is, returning a  $d \times d$  matrix) with complexity

$$O((\xi_H + \rho_q d^8 \log d \log \log d \log q) \log \epsilon^{-1}).$$

We prove Theorem 1.1 over the course of the paper, by describing explicitly the steps of the algorithm. This is a very specialised algorithm which provides a major improvement over the runtimes of the existing best algorithms (although the existing algorithms remain extremely useful, for they apply in many more cases than this one).

$G$	Minimum $d$	Conditions
$\mathrm{SL}(d, q)$	3	–
$\mathrm{SU}(d, q)$	3	$d$ odd
	4	$d$ even
$\mathrm{Sp}(d, q)$	6	$d$ even
$\mathrm{SO}^-(d, q)$	6	$d$ even
$\mathrm{SO}^\circ(d, q)$	7	$d$ odd
$\mathrm{SO}^+(d, q)$	8	$d$ even

TABLE 1. Minimum values of  $d$  for **Initialise**

## 2. MODULES AND REPRESENTATIONS

In this section we introduce some notation, in particular the Symmetric Square module and its irreducible constituents (note that in many cases, the Symmetric Square is itself irreducible). Let  $V = V(d, q)$  be a vector space over a field  $F = \mathbb{F}_q$  of order  $q$ . Then  $V$  is called an  $FG$ -module if the group  $G$  acts on  $V$  in a way compatible with the vector space structure of  $V$ : that is, if  $(v + w)^g = v^g + w^g$  and  $(av)^g = av^g$  for all  $g \in G, v, w \in V, a \in F$ . An  $FG$ -submodule is a subspace of  $V$  left invariant by the action of  $G$ : an *irreducible  $FG$ -module* is a module with no proper nontrivial submodules. When a group  $G$  acts on several  $FG$ -modules, we use a subscript where necessary to distinguish the actions (for example,  $g_V$  denotes the action of  $g \in G$  on an  $FG$ -module  $V$ ). For two  $FG$ -modules  $V, W$  with bases  $\{v_1, \dots, v_{d_1}\}, \{w_1, \dots, w_{d_2}\}$ , the *tensor product*  $V \otimes W$  is the  $FG$ -module with basis  $\{v_i \otimes v_j \mid 1 \leq i \leq d_1, 1 \leq j \leq d_2\}$ : an element  $g \in G$  acts in the diagonal way  $(v \otimes w)^g = v^g \otimes w^g$  (extending by linearity, this gives an  $FG$ -module structure).

Consider an extension  $K := \mathbb{F}_{q^{d'}}$  of  $F := \mathbb{F}_q$ , and fix a basis  $\{v_1, \dots, v_d\}$  of  $V$ . Then viewing  $K$  as an  $F$ -vector space (and, in turn, an  $FG$ -module with  $G$  acting trivially), the tensor product  $V \otimes K$  is isomorphic to the  $K$ -vector space with basis  $\{v_1, \dots, v_d\}$ , with the same  $G$ -action. We denote this module by  $V_K$ , and observe that all properties of  $g \in G$  carry over in this action: in particular, the characteristic polynomial does not change, although its irreducible factors do, since the notion of irreducibility of a polynomial depends upon the field. By considering the action of  $g$  on  $V_K$ , we may access a richer eigenstructure.

**2.1. The Symmetric Square  $S^2(V)$ .** The Symmetric Square module  $S^2(V)$  is an irreducible constituent of the tensor square  $V \otimes V$ : let  $G \in \mathrm{GL}(V)$ , and let  $\{v_i \mid 1 \leq i \leq d\}$  be a basis for  $V$ . The *Symmetric Square Module*  $S^2(V)$  is the  $FG$ -submodule of  $V \otimes V$  generated by

$$\{v_i \otimes v_i \mid 1 \leq i \leq d\} \cup \{v_i \otimes v_j + v_j \otimes v_i \mid 1 \leq i < j \leq d\}.$$

Since  $(-v) \otimes (-w) = v \otimes w$ , the element  $-1 \in G$  acts trivially on  $V \otimes V$  (and hence on  $S^2(V)$ ). In fact, the set  $\{\pm 1\}$  is precisely the kernel of this action. For this reason, our rewriting algorithm can only return the action on  $V$  modulo this kernel. Our primary method for the rewriting algorithm is the analysis of the eigenvalues and eigenspaces of a group element. Since the eigenstructure of a group element depends on its action on a vector space, an element  $g$  will usually have different

eigenstructures, depending on whether we consider  $g_V, g_{V \otimes V}, g_{S^2(V)}$  or an action on another module, and also depending on the underlying field (note that when the field changes, the characteristic polynomial will not change: however, its roots might!). We now present several relationships between the eigenstructures of an element  $g \in G$  in its action on different modules. Let  $F = \mathbb{F}_q$ , let  $K = \mathbb{F}_{q^{d'}}$  for some integer  $d'$ , let  $V = F^d$ , and suppose that  $g \in \text{GL}(d, q)$  has  $d$  (not necessarily distinct) eigenvalues  $\{\lambda_i \mid 1 \leq i \leq d\}$  in its action on  $V_K$ , and there exists a basis  $\{v_1, \dots, v_d\}$  for  $V_K$  of  $g$ -eigenvectors (so that for each  $i$ ,  $v_i g = \lambda_i v_i$ ). Then the eigenvalues of  $g$  in its action on  $(V \otimes_F V)_K$  are

$$\{\lambda_i \lambda_j \mid 1 \leq i \leq j \leq d\},$$

and for each  $i, j$ , both  $v_i \otimes v_j$  and  $v_j \otimes v_i$  are  $(\lambda_i \lambda_j)$ -eigenvectors in  $(V \otimes_F V)_K$ . Moreover, these are the only eigenvalues of  $g$  in  $(V \otimes V)_K$ .

**Lemma 2.1.** *Let  $g \in \text{GL}(V)$ , and suppose that  $g$  has eigenvalues  $\lambda_1, \dots, \lambda_d$  in its action on  $V$ , and that  $\{v_1, \dots, v_d\}$  is a basis for  $V$  such that for all  $i$ ,  $v_i$  is a  $\lambda_i$ -eigenvector for  $g_V$ . Let  $v_{ij} = v_i \otimes v_j + v_j \otimes v_i$  when  $i \neq j$ , and  $v_{ii} = v_i \otimes v_i$ . Then*

$$\{v_{ij} \mid 1 \leq i \leq j \leq d\}$$

*is a basis for  $S^2(V)$ , such that for every  $i, j$ ,  $v_{ij}$  is a  $(\lambda_i \lambda_j)$ -eigenvector for  $g$  in its action on  $S^2(V)$ .*

*Proof.* By the comments above, both  $v_i \otimes v_j, v_j \otimes v_i$  are  $(\lambda_i \lambda_j)$ -eigenvectors of  $g_{V \otimes V}$ , and so any linear combination of the two is itself a  $(\lambda_i \lambda_j)$ -eigenvector. That this set forms a basis is clear by comparing dimensions.  $\square$

We often consider the matrix of a given  $g \in G$  in its action on multiple bases. For this reason we introduce the following notation: if  $g \in G$  and  $\mathcal{B}$  is an ordered basis for  $V$ , then  $g_{\mathcal{B}}$  denotes the matrix of  $g$  with respect to  $\mathcal{B}$ ; if  $b_i, b_j \in \mathcal{B}$  then and  $g_{b_i b_j}$  denotes the coefficient of  $b_2$  in the expansion of  $b_1^g$  (in the case that our basis is indexed in the usual way, this is the  $(i, j)$ -entry of  $g_{\mathcal{B}}$ ).

Let  $V$  be an  $FG$ -module, and let  $\mathcal{B} := \{b_i \mid 1 \leq i \leq d\}, \mathcal{B}' = \{b'_i \mid 1 \leq i \leq d\}$  be bases for  $V$ , such that for every  $i$ , there exists  $c_i \in F^* := F \setminus \{0\}$  such that  $b'_i = c_i b_i$ . Then for every  $g \in G$  and for all  $i, j$ , we have  $g_{b'_i b'_j} = \frac{c_i}{c_j} g_{b_i b_j}$ . If  $\varphi : V \rightarrow W$  is an isomorphism of  $FG$ -modules and  $\mathcal{V}$  is a basis for  $V$ , then  $\mathcal{V}^\varphi$  is a basis for  $W$ , and for all  $v, w \in \mathcal{V}, g \in G$ , we have  $g_{v^\varphi w^\varphi} = g_{vw}$ .

If instead  $W$  is a  $G$ -invariant subspace of  $V$ , then the quotient space  $V/W := \{v + W \mid v \in V\}$  is an  $FG$ -module of dimension  $\dim V - \dim W$ , with the action of  $g \in G$  defined by  $(v + W)^g = v^g + W$ . Moreover, suppose that  $\text{quo}_W : V \rightarrow V/W$  is the natural quotient map  $v \mapsto v + W$ , and  $e, f \in V$  are basis vectors such that  $\langle e, f \rangle \cap W = \{0\}$ . Then for every  $g \in G$ , we have that  $g_{e, f} = g_{\text{quo}(e), \text{quo}(f)}$ . Finally suppose that  $e, f \in \mathcal{V}$  are basis vectors such that  $e, f \in W$ . Then for every  $g \in G$ , we have that  $g_{ef} = (g_W)_{ef}$ . Just as we may seek normal subgroups of groups by defining homomorphisms and inspecting their kernels, we will construct submodules of  $FG$ -modules by considering the nullspaces of certain maps: if  $T$  is a  $G$ -invariant linear form on an  $FG$ -module  $W$ , then the kernel of  $T$  is an  $FG$ -submodule of  $W$ .

**Lemma 2.2.** *Let  $G$  be a group,  $W$  be an  $FG$ -module, and let  $T$  be a  $G$ -invariant linear form on  $W$  (that is, a linear map  $W \rightarrow F$ ), and let  $g \in G$ . If  $g_W$  has an eigenvalue  $\lambda \neq 1$  in  $F$ , then the  $\lambda$ -eigenspace of  $g$  is contained in the kernel of  $T$ .*

Given the matrix of a group element  $g \in G$  in its action on a module  $V$  with respect to a fixed basis (as is always the case when dealing with a computer representation of a group), we may easily construct corresponding matrices for the actions of  $g$  on  $V \otimes V$  and  $S^2(V)$ :

**Lemma 2.3.** *Let  $G \leq \text{GL}(V)$ , and let  $\mathcal{V} := \{v_i \mid 1 \leq i \leq d\}$  be a basis for  $V$ . Let  $g \in G$ , and write  $g_{ij} = g_{v_i v_j}$ . Define  $v_{ij}$  as in Lemma 2.1. Then*

- (i)  $g_{v_i \otimes v_j, v_k \otimes v_\ell} = g_{ik} g_{j\ell}$ , for any  $i, j, k, \ell \in [1 \dots d]$ ; and
- (ii) for  $1 \leq i \leq j \leq d, 1 \leq k \leq \ell \leq d$ , we have

$$g_{v_{ij}, v_{k\ell}} = g_{ik} g_{j\ell} + (1 - \delta_{k\ell}) g_{i\ell} g_{jk}.$$

*Proof.* By definition we have

$$\begin{aligned} (v_i \otimes v_j)^g &= v_i^g \otimes v_j^g = \left( \sum_{k=1}^d g_{ik} v_k \right) \otimes \left( \sum_{\ell=1}^d g_{j\ell} v_\ell \right) \\ &= \sum_{k=1}^d \sum_{\ell=1}^d (g_{ik} g_{j\ell}) v_k \otimes v_\ell, \end{aligned}$$

and (i) follows. For (ii), observe that, for  $i \neq j$ , we have

$$\begin{aligned} (v_i \otimes v_j + v_j \otimes v_i)^g &= v_i^g \otimes v_j^g + v_j^g \otimes v_i^g \\ &= \sum_{k=1}^d \sum_{\ell=1}^d (g_{ik} g_{j\ell} + g_{jk} g_{i\ell}) v_k \otimes v_\ell \end{aligned}$$

Since switching  $k, \ell$  does not change the value of  $g_{ik} g_{j\ell} + g_{jk} g_{i\ell}$ , we have

$$(v_i \otimes v_j + v_j \otimes v_i)^g = \sum_{k=1}^d \sum_{\ell \geq k}^d (g_{ik} g_{j\ell} + g_{jk} g_{i\ell}) (v_k \otimes v_\ell + v_\ell \otimes v_k).$$

The proof when  $i = j$  follows by an identical argument.  $\square$

### 3. SPECIAL ELEMENTS AND THEIR EIGENSTRUCTURE

**3.1. Singer Cycles (Motivation).** In [14], Magaard, O'Brien & Seress exploit the eigenstructure of Singer Cycles in  $G = \text{SL}(d, q)$  in their action on small degree  $\mathbb{F}_q G$ -modules to produce their algorithm for rewriting. In other Classical groups, such elements cannot always be found. A *Special Element* has many of the same properties: in essence we define a Special Element as a ‘good enough analogue’ to the elements exploited in [14]. Special elements act irreducibly on a subspace of  $V$  of large dimension, and have large order (in both of these respects, the meaning of ‘large’ is dependent on our needs).

Let  $q$  be a prime power, and  $d$  a positive integer. Then a prime  $r$  is called a *primitive prime divisor* (ppd) of  $q^d - 1$  if  $r \mid (q^d - 1)$ ; and for  $1 \leq e < d$ , we have  $r \nmid (q^e - 1)$ . A *Singer Cycle* in  $\text{GL}(d, q)$  is an element of order  $q^d - 1$ : we identify such elements with primitive elements of the extension field  $\mathbb{F}_{q^d}$ . For  $1 \leq d' \leq d$ , An element  $s \in \text{GL}(d, q)$  is called a  $\text{ppd}(d, q; d')$ -element if  $o(s)$  is divisible by a

primitive prime divisor of  $q^{d'} - 1$ .

If  $s$  is a  $\text{ppd}(d, q; d')$ -element, then the characteristic polynomial  $c_s(t)$  of  $s$  has an irreducible divisor  $f$  of degree  $d'$ , and acts irreducibly on a unique  $d'$ -dimensional subspace  $V_f$  of  $V$  (the  $f$ -primary component of  $V$  [5]): in the case of Singer Cycles,  $c_s(t)$  is irreducible and  $V_f = V$ . Some subgroups of  $\text{GL}(d, q)$  have no Singer Cycles, and so we must settle for  $d'$  as large as possible (in the worst case,  $d' = d - 2$ ).

The fact that  $c_s(t)$  has a high degree irreducible divisor may seem, at first, bad news for any attempt to exploit the eigenstructure of  $s$  – after all, eigenvalues will arise when the divisors of  $c_s(t)$  have *smallest* degree, not largest. However, an irreducible divisor of  $c_s(t)$  of degree  $d'$  gives rise to  $d'$  distinct eigenvalues in the action of  $s$  on  $V_K = V \otimes K$ , where  $K = \mathbb{F}_{q^{d'}}$ . Moreover, these distinct eigenvalues (and, consequently, their eigenvectors) form an orbit of the action of the Frobenius map  $\sigma : x \mapsto x^q$  of the extension  $K/F$ .

**Lemma 3.1.** *If  $s \in \text{GL}(d, q)$  acts irreducibly on  $V$ , then the eigenvalues of  $s$  on  $V_K$  are*

$$\{\ell_i = \lambda^{q^{i-1}} \mid 1 \leq i \leq d\}$$

for some  $\lambda \in K$  with  $o(\lambda) = o(s)$ , and there exists a basis  $\mathcal{E}(s, V) := \{e_i \mid 1 \leq i \leq d\}$  of  $V_K$  such that for all  $i$ , we have that  $\langle e_i \rangle$  is the eigenspace of  $\ell_i$ , and  $e_i^\sigma = e_{i+1}$  for every  $i \in [1 \dots d - 1]$ , and  $e_d^\sigma = e_1$ . That is, we have  $e_i^\sigma = e_{\text{res}_d(i+1)}$ , for all  $i$ .

*Proof.* By [12, Theorem 2.14], since the characteristic polynomial of  $s$  is irreducible of degree  $d$  over  $F$ , the eigenvalues of  $s$  in  $V_K$  (which are precisely the roots in  $K$  of the characteristic polynomial of  $s$ ) are as asserted and the  $\ell_i$  are distinct. Thus there are  $d$  eigenspaces of dimension 1 in  $V_K$ . Fix an eigenvector  $e_1$  of  $\ell_1$ , such that the first nonzero entry of  $e_1$  is 1, and for each  $i$  with  $2 \leq i \leq d$ , set  $e_i := e_1^{q^{i-1}}$ . Then for each  $i$ , since  $s \in \text{GL}(V_F)$  and is therefore fixed under the action of  $\sigma$ :

$$e_i^s = e_1^{\sigma^{i-1}s} = (e_1 s)^{\sigma^{i-1}} = (\ell_1 e_1)^{\sigma^{i-1}} = \ell_1^{q^{i-1}} e_i = \ell_i e_i,$$

and so  $e_i$  is an  $\ell_i$ -eigenvector for  $s$  as required.

Moreover, since  $\ell_d^q = \lambda^{q^d} = \lambda = \ell_1$ , we have that  $e_d^\sigma \in \langle e_1 \rangle$ , that is,  $e_d^\sigma$  is a scalar multiple of  $e_1$ . Since  $e_1$  has its first nonzero coordinate equal to 1, and since the action of  $\sigma$  fixes this coordinate, we have  $e_d^\sigma = e_1$ .  $\square$

**Corollary 3.2.** *Let  $s \in \text{GL}(d, q)$ , and suppose that there exists a  $d'$ -dimensional  $s$ -invariant subspace  $U$  of  $V$ , such that  $s$  acts irreducibly on  $U$ . Then  $s|_U$  has  $d'$  eigenspaces of dimension 1 in  $U_K$ , and there exists a basis  $\mathcal{E} = \{e_i \mid 1 \leq i \leq d'\}$  for  $U_K$  such that  $e_i^\sigma = e_{\text{res}_{d'}(i+1)}$ .*

**Definition 3.3.** Let  $G$  be a classical group of rank  $r$  as in one of the lines of Table 2. Let  $d'$  be as in the 4th column of the corresponding line of Table 2. Then an element  $s \in G$  is a *special element* if  $s$  is a  $\text{ppd}(d, q; d')$ -element, and there exists an  $s$ -invariant decomposition  $V = U \oplus U'$  such that  $\dim U = d'$ ; and  $o(s|_U)$  is a multiple of the value in the 5th column of the appropriate line of Table 2; and if  $d' < d$ , then  $o(s|_{U'})$  is equal to the value in the 6th column of the appropriate line of Table 2.

Case	$d$	$G$	$d'$	$o(s _U)$	$o(s _{U'})$	Conditions
$A_r$	$r+1$	$\mathrm{SL}(d, q)$	$d$	$\frac{q^d - 1}{q - 1}$	–	–
${}^2A_r$	$r+1$	$\mathrm{SU}(d, q)$	$d$	$\frac{\sqrt{q}^d + 1}{\sqrt{q} + 1}$	–	$d$ odd, $q$ square
			$d-1$	$\frac{\sqrt{q}^{d'} + 1}{\sqrt{q} + 1}$	1	$d$ even, $q$ square
$B_r$	$2r+1$	$\mathrm{SO}(d, q)$	$d-1$	$q^{d'/2} + 1$	1	–
$C_r$	$2r$	$\mathrm{Sp}(d, q)$	$d$	$q^{d'/2} + 1$	–	–
$D_r$	$2r$	$\mathrm{SO}^+(d, q)$	$d-2$	$q^{d'/2} + 1$	$q+1$	–
${}^2D_r$	$2r$	$\mathrm{SO}^-(d, q)$	$d$	$q^{d'/2} + 1$	–	–

TABLE 2. Properties of Special Elements of Classical Groups

**Remark 3.4.** We frequently refer to our procedure **Initialise** ‘searching for special elements’, but this is not strictly true. Special elements, as in Definition 3.3, are merely a *subset* of the elements that **Initialise** can use: in practice we may use elements with smaller order than the values in Table 2 (i.e. certain powers of special elements), but the proof that such elements are suitable is neither interesting nor illuminating, and adds no value to the analysis of our algorithms. In practice we may essentially ‘replace’ the appearances of  $q^{d'/2} + 1$  in Table 2 with  $\frac{q^{d'/2} + 1}{\gcd(q+1, q^{d'/2} + 1)}$ .

The subspace  $U$  in Definition 3.3 is uniquely determined by  $s$ , and  $s$  acts irreducibly on  $U$ ; if  $d' < d$ , then  $s$  also acts irreducibly on  $U'$  as a consequence of the condition on  $o(s|_{U'})$ . Our ultimate goal is a basis for  $V_L$ , where  $L$  is an extension field of  $F$  satisfying certain conditions: we define these conditions below.

**Definition 3.5.** Let  $G$  be a classical group over  $F$ , let  $V$  be the natural  $FG$ -module, and let  $\sigma$  be the Frobenius automorphism of  $K/F$ , where  $K$  is an extension of  $F$  of degree  $d'$  as given in Table 2. Let  $\mathcal{F} := \{f_i \mid 1 \leq i \leq d\}$  be a basis for  $V$ : then we say  $\mathcal{F}$  *satisfies the almost- $\sigma$ -relations for  $V$*  if the following hold:

- (i) for  $1 \leq i \leq d' - 1$ , we have that  $f_i^\sigma = f_{i+1}$ , and  $f_{d'}^\sigma \in \langle f_1 \rangle$ ;
- (ii) if  $d' = d - 1$ , then  $f_d^\sigma = f_d$ ; and
- (iii) if  $d' = d - 2$ , then  $f_{d-1}^\sigma = f_d$  and  $f_d^\sigma = f_{d-1}$ .

If, in addition, we have  $f_{d'}^\sigma = f_1$ , then we say  $\mathcal{F}$  *satisfies the  $\sigma$ -relations for  $V$* .

We now describe explicitly the eigenstructure of a special element on  $V_K$ :

**Lemma 3.6.** *Let  $G$  be a classical group of rank  $r$ , let  $d'$  be as in Table 2, and let  $s \in G$  be a special element. Let  $K = \mathbb{F}_{q^{d'}}$ , and let  $U, U'$  be as in Definition 3.3. Then the eigenvalues of  $s$  in its action on  $V_K$  are*

$$\{\ell_i \mid 1 \leq i \leq d\},$$

where

$$\ell_i = \begin{cases} \lambda^{q^{i-1}} & \text{for } 1 \leq i \leq d', \\ \mu^{q^{i-d'}-1} & \text{for } d' < i \leq d, \end{cases}$$

for  $\lambda, \mu \in K$  satisfying  $\lambda = o(s|_U), \mu = o(s|_{U'})$  as in the 5th and 6th entry respectively in the appropriate line of Table 2. Moreover, there exists a basis

$$\mathcal{E} := \mathcal{E}(s, V) := \{e_i := e_{s, V, i} \mid 1 \leq i \leq d\}$$

such that  $\mathcal{E}$  satisfies the  $\sigma$ -relations for  $V$  as in Definition 3.5.

*Proof.* If  $d' = d$  then the result follows immediately from 3.1. If  $d' = d - 1$ , then by definition we have  $o(s|_{U'}) = 1$ , and so  $s$  acts trivially on  $U'$ : that is,  $\ell_d = 1$  is an eigenvalue of  $s$ , and the result follows from this fact and Corollary 3.2, since  $s$  acts irreducibly on both  $U$  and  $U'$ .

If  $d' = d - 2$ , then  $s|_{U'} \in \text{GL}(2, q)$  has order  $q + 1$ , and hence acts irreducibly on  $U'$  (since all proper nontrivial subspaces of  $U'$  are 1-dimensional), and the result follows by applying Corollary 3.2 separately to  $U$  and  $U'$ .  $\square$

#### 4. ARITHMETIC

In this section we prove a series of results in modular arithmetic which will be used in Section 5 below. These results have been separated so that the later results, which are more relevant in the bigger picture, are not obfuscated by these long, repetitive and technical proofs.

By Lemma 2.1, the multiset of eigenvalues of a special element of a classical group  $G$  in its action on the tensor product  $(V \otimes_F V)_K$  is the multiset

$$\Sigma := \{\ell_{ij} \mid i, j \in \{1, \dots, d\}\},$$

where each  $\ell_{ij}$  is an element of  $K = \mathbb{F}_{q^{d'}}$ , and is the product of a pair of eigenvalues of  $s$  in its action on  $V_K$  as described in Lemma 5.11 below (note that the details of this are not required for the results in this section, except as motivation). This multiset has size  $d^2$ , but contains repeated values: in all cases, for example, we have  $\ell_{ij} = \ell_{ji}$ . In this section we provide necessary conditions for other coincidences to occur.

**Proposition 4.1.** *Suppose  $q$  is a prime power, that  $d' \in \mathbb{Z}$  with  $d' \geq 4$ , and suppose there exists  $j, m, n \in \mathbb{Z}$ , with  $1 \leq j \leq d'/2$ ,  $1 \leq m < n \leq d'$  and satisfying*

$$(1) \quad 1 + q^{j-1} - q^{m-1} - q^{n-1} \equiv 0 \pmod{\frac{q^{d'} - 1}{q - 1}}.$$

*Then  $m = 1$  and  $n = j$ .*

*Proof.* For all such  $j, m, n$ , we have

$$1 + q^{j-1} - q^{m-1} - q^{n-1} \leq 1 + q^{d'/2-1} - 1 - 1 = -1 + q^{d'/2} < \frac{q^{d'} - 1}{q - 1},$$

and on the other hand,

$$1 + q^{j-1} - q^{m-1} - q^{n-1} \geq 2 - q^{d'-1} - q^{d'-2} = -\frac{q^{d'} - q^{d'-2} + 2 - 2q}{q - 1} > -\frac{q^{d'} - 1}{q - 1}$$

and so we have equality in (1), not just equivalence modulo  $\frac{q^{d'} - 1}{q - 1}$ . Thus

$$1 + q^{j-1} = q^{m-1} + q^{n-1}$$



and reducing modulo  $q$  we have that  $m = 1$ , from which it immediately follows that  $n = j$ .  $\square$

We now address the ‘hard case’, where  $d'$  is even and  $o(\lambda)$  is  $q^{d'/2} + 1$ . We seek solutions to the equation

$$(2) \quad 1 + q^{j-1} + \epsilon_m q^{m'-1} + \epsilon_n q^{n'-1} = t(q^{d'/2} + 1)$$

for integer values of  $j, m', n', \epsilon_m, \epsilon_n, t$  with  $1 \leq j, m', n' \leq d'/2$ ,  $\epsilon_m, \epsilon_n \in \{-1, 1\}$ . We make an important distinction here: due to the fact that the Symmetric Square module contains the Alternating Square module when  $q$  is even (and therefore we do not consider it in this paper), we *need not consider* the case that  $j = 1$  when  $q$  is even. For completeness (and for future use) we still consider the cases that apply to the Alternating Square (i.e.  $q$  even and  $j \neq 1$ ).

**Lemma 4.2.** *Suppose  $q$  is a prime power, that  $d' \in \mathbb{Z}$  is even with  $d' \geq 6$ , and suppose that  $j, m', n', \epsilon_m, \epsilon_n, t \in \mathbb{Z}$ , with  $1 \leq j, m', n' \leq d'/2$ ,  $\epsilon_m, \epsilon_n \in \{\pm 1\}$ , and  $(m', \epsilon_m) \neq (n', \epsilon_n)$ , satisfy (2).*

*Then  $t \in \{0, 1\}$ , and if  $t = 1$  then  $q = 2$ , and up to switching  $m, n$ , we have that  $j = \frac{d'}{2} - 1, \epsilon_m = 1, m' = \frac{d'}{2} - 1, \epsilon_n = 1, n' = \frac{d'}{2}$ .*

*Proof.* Since the pair  $(m', \epsilon_m) \neq (n', \epsilon_n)$ , we have

$$2 - q^{d'/2-1} - q^{d'/2-2} \leq 1 + q^{j-1} + \epsilon_m q^{m'-1} + \epsilon_n q^{n'-1} \leq 1 + q^{d'/2-2} + 2q^{d'/2-1},$$

and so

$$\frac{2 - q^{d'/2-1} - q^{d'/2-2}}{q^{d'/2} + 1} \leq t \leq \frac{1 + q^{d'/2-2} + 2q^{d'/2-1}}{q^{d'/2} + 1}.$$

It is readily checked that the upper bound is less than 1 if  $q \geq 3$ , and less than 2 if  $q = 2$ , while the lower bound is greater than  $-1$  for all  $q$ . Suppose that  $t = 1$ : then  $q = 2$  (we continue to write  $q$ ), and (2) is

$$1 + q^{j-1} + \epsilon_m q^{m'-1} + \epsilon_n q^{n'-1} = q^{d'/2} + 1.$$

Now the largest value the left hand side can take is when  $j = d'/2, \epsilon_m = \epsilon_n = 1, m' = d'/2 - 1, n' = d'/2$ , and in this case we have

$$1 + q^{j-1} + \epsilon_m q^{m'-1} + \epsilon_n q^{n'-1} = 1 + 2q^{d'/2-1} + q^{d'/2-2} = 1 + q^{d'/2} + q^{d'/2-2} > 1 + q^{d'/2}.$$

The next-largest value is attained when  $j = d'/2 - 1, \epsilon_m = \epsilon_n = 1, m' = d'/2 - 1, n' = d'/2$ : in this case

$$1 + q^{j-1} + \epsilon_m q^{m'-1} + \epsilon_n q^{n'-1} = 1 + 2q^{d'/2-2} + q^{d'/2-1} = 1 + 2q^{d'/2-1} = 1 + q^{d'/2}.$$

This is precisely the solution given. All *other* combinations of  $j, \epsilon_m, m', \epsilon_n, n'$  give smaller values for the left hand side, and so cannot yield solutions.  $\square$

**Proposition 4.3.** *Suppose  $q$  is a prime power, that  $d' \in \mathbb{Z}$  is even with  $d' \geq 6$ , and suppose that  $j, m', n', \epsilon_m, \epsilon_n \in \mathbb{Z}$ , with  $1 \leq j, m', n' \leq d'/2$ ,  $\epsilon_m, \epsilon_n \in \{\pm 1\}$ , and  $(m', \epsilon_m) \neq (n', \epsilon_n)$ , satisfy*

$$(3) \quad 1 + q^{j-1} + \epsilon_m q^{m'-1} + \epsilon_n q^{n'-1} \equiv 0 \pmod{q^{d'/2} + 1}.$$

*Then one of the following holds:*

- (i)  $\epsilon_m = \epsilon_n = -1$  and  $\{1, j\} = \{m', n'\}$  (the trivial solution);
- (ii)  $q = 2, j = \frac{d'}{2} - 1, \epsilon_m = 1, m' = \frac{d'}{2} - 1, \epsilon_n = 1, n' = \frac{d'}{2}$ .

- (iii)  $q = 3, j = 1, m' = \epsilon_m = 1, n' = 2, \epsilon_n = -1$ ; or
- (iv)  $q = 2, j = 2, m' = \epsilon_m = 1, n' = 3, \epsilon_n = -1$ .

*Proof.* Suppose that we are not in case (ii): then by Lemma 4.2, we have equality in (3). Reducing modulo  $q$  we have

$$(4) \quad 1 + q^{j-1} + \epsilon_m q^{m'-1} + \epsilon_n q^{n'-1} \equiv 0 \pmod{q}.$$

Since  $(m', \epsilon_m) \neq (n', \epsilon_n)$  implies  $\epsilon_m q^{m'-1} \neq \epsilon_n q^{n'-1}$ , they cannot both be 1 nor both  $-1$ , and so the left hand side of (4), when reduced modulo  $q$ , is equal to 0, 1, 2 or 3. Since  $q \geq 2$ , only the values 0, 2 and 3 can possibly be equivalent to 0 modulo  $q$ . We treat each case separately, and refer to the value of the left hand side of (4) after it has been reduced modulo  $q$  as the *reduced left hand side* of (4).

If the reduced left hand side of (4) is 3, then  $q = 3, j = 1$  and exactly one of  $\epsilon_m q^{m'-1}, \epsilon_n q^{n'-1} = 1$ , say  $m' = \epsilon_m = 1$  and  $n' > 1$ . Then (2) yields

$$3 + \epsilon_n q^{n'-1} = 0,$$

forcing  $\epsilon_n = -1, n' = 2$ : This is solution (ii).

If the reduced left hand side of (4) is 2, then  $q = 2$  and one of the terms in the left hand side is 1, say  $\epsilon_m q^{m'-1} = 1$  (noting that when  $q$  is even we have  $j > 1$ ). Then (2) is

$$2 + q^{j-1} + \epsilon_n q^{n'-1} = 0,$$

forcing  $\epsilon_n = -1$ , and so

$$2 + q^{j-1} = q^{n'-1}.$$

There is only one way in which ‘2 plus a power of 2’ can equal a power of 2: namely  $2 + 2 = 4$ , and so  $j = 2, n' = 3$ . This is solution (iii).

Finally, if the reduced left hand side of (4) is zero, then  $j \geq 2$  and one of  $\epsilon_m q^{m'-1}, \epsilon_n q^{n'-1} = -1$ , say  $m' = 1, \epsilon_m = -1$  and  $n' > 1$ . Then (2) reduces to

$$q^{j-1} + \epsilon_n q^{n'-1} = 0,$$

and so  $\epsilon_n = -1, n' = j$ . Thus  $m = 1, j = n, \epsilon_m = \epsilon_n = -1$ , the trivial solution.  $\square$

In the case  $G = \text{SU}(d, q)$ , we have that  $q$  is a square, and  $\lambda$  has smaller order than  $q^{d'/2} + 1$ , and so we must treat it separately (though we use similar methods), and we must solve the following equation, which bears a strong similarity to (2): note that in the Unitary case, we have  $d'$  odd.

**Proposition 4.4.** *Suppose  $q$  is a square prime power, that  $d' \in \mathbb{Z}$  with  $d' \geq 3$ , and suppose that  $j, m', n', \epsilon_m, \epsilon_n \in \mathbb{Z}$ , with  $1 \leq j, m', n' \leq (d' - 1)/2$ ,  $\epsilon_m, \epsilon_n \in \{\pm 1\}$ , and  $(m', \epsilon_m) \neq (n', \epsilon_n)$ , satisfy*

$$(5) \quad 1 + q^{j-1} + \epsilon_m q^{m'-1} + \epsilon_n q^{n'-1} \equiv 0 \pmod{\frac{\sqrt{q}^{d'} + 1}{\sqrt{q} + 1}}$$

*Then  $\epsilon_m = \epsilon_n = -1$  and  $\{1, j\} = \{m', n'\}$ .*

*Proof.* Suppose that

$$1 + q^{j-1} + \epsilon_m q^{m'-1} + \epsilon_n q^{n'-1} = t \left( \frac{\sqrt{q}^{d'} + 1}{\sqrt{q} + 1} \right).$$

Now since the pair  $(m', \epsilon_m) \neq (n', \epsilon_n)$ , we have

$$2 - q^{(d'-1)/2-1} - q^{(d'-1)/2-2} \leq 1 + q^{j-1} + \epsilon_m q^{m'-1} + \epsilon_n q^{n'-1} \leq 1 + q^{(d'-1)/2-2} + 2q^{(d'-1)/2-1},$$

and so

$$\frac{q^{1/2} + 1}{q^{d'/2} + 1} \left( 2 - q^{(d'-1)/2-1} - q^{(d'-1)/2-2} \right) \leq t \leq \frac{q^{1/2} + 1}{q^{d'/2} + 1} \left( 1 + q^{(d'-1)/2-2} + 2q^{(d'-1)/2-1} \right).$$

Onve again it is simple to check (noting that  $q \geq 4$ ) that the left hand side is greater than  $-1$ , while the right hand side is less than  $1$ . Thus  $t = 0$  and we have equality in (5), and the result follows by the arguments in the proof of Proposition 4.3, noting that the exceptional cases with  $q$  not a square do not arise.  $\square$

For the sake of brevity we state the remaining results of this Section without proof: the statements and analysis are similar to the results above, and the full proofs (as well as more detailed proofs of the results above) are available in Section 2.4 of [3] (we will refer the reader to the specific results as we go).

**Proposition 4.5** ([3], Proposition 2.4.13). *Suppose  $q$  is a prime power, that  $d' \geq 8$ , and suppose that  $t, j, m', \epsilon_m \in \mathbb{Z}$ , with  $1 \leq j, m' \leq d'/2$ ,  $\epsilon_m \in \{\pm 1\}$ , satisfy*

$$(6) \quad 1 + q^{j-1} + \epsilon_m q^{m'-1} \equiv 0 \pmod{q^{d'/2} + 1}.$$

*Then  $q = 2$ , and one of the following holds:*

- (i)  $d' = 10, j = 3, \epsilon_m = -1, m' = 5$  (that is,  $3 \times (1 + 4 - 16) = -32 - 1$ );
- (ii)  $j = 1, \epsilon_m = -1, m' = 2$  (that is,  $3 \times (1 + 1 - 2) = 0$ ); or
- (iii)  $d' = 10, \epsilon_m = 1, \{j, m'\} = \{2, 4\}$  (that is,  $3 \times (1 + 2 + 8) = 32 + 1$ ).

Proposition 4.5 solves the issue of whether eigenvalues of the form  $\ell_{ij}, \ell_s m_t$  can be equal, in the case  $d' = d - 2$  below. In the case  $d' = d - 1$ , we must compare eigenvalues of the form  $\ell_{ij}, \ell_m$ :

**Corollary 4.6** ([3], Corollary 2.4.14). *Suppose  $q$  is a prime power, that  $d' \geq 8$ , and suppose that  $j, m', \epsilon_m \in \mathbb{Z}$ , with  $1 \leq j, m' \leq d'/2$ ,  $\epsilon_m \in \{\pm 1\}$ , satisfy*

$$(7) \quad 1 + q^{j-1} + \epsilon_m q^{m'-1} \equiv 0 \pmod{q^{d'/2} + 1}.$$

*Then  $q = 2, j = 1, \epsilon_m = -1, m' = 2$ .*

*Proof.* Multiplying by  $(q + 1)$  implies that (6) holds, and so the result immediately follows by testing the solutions found in Proposition 4.5: of these, only (ii) satisfies (7).  $\square$

Once again we must treat the Unitary case separately:

**Corollary 4.7** ([3], Corollary 2.4.15). *Suppose  $q$  is a square prime power, that  $d' \geq 5$ . Then there is no  $j, m', \epsilon_m \in \mathbb{Z}$ , with  $1 \leq j, m' \leq (d' - 1)/2$ ,  $\epsilon_m \in \{\pm 1\}$ , satisfying*

$$(8) \quad 1 + q^{j-1} + \epsilon_m q^{m'-1} \equiv 0 \pmod{\frac{\sqrt{q}^{d'} + 1}{\sqrt{q} + 1}}.$$

### 5. THE EIGENSTRUCTURE OF SPECIAL ELEMENTS ON $(V \otimes V)_K$

In this section we determine the precise eigenstructure of a special element  $s \in G$  in its action on  $(V \otimes V)_K$ , which will enable us to determine the eigenstructure of  $s$  in its action on  $S^2(V)_K$ . This eigenstructure is the crux of the procedures **Initialise** and **FindPreimage**. Throughout this section, define  $\text{res}_{d'}(i)$  as the unique integer  $j$  such that  $1 \leq j \leq d'$  and  $j \equiv i \pmod{d'}$ .

**5.1. Coincident Eigenvalues**  $\ell_{ij}$ . There are two ways in which eigenvalues  $\ell_{ij}$  may coincide: there are cases where  $\ell_{ij} = 1$  (leading to a nontrivial fixed-point space of  $s$ ), or where two eigenvalues are not 1, but coincide anyway.

**Lemma 5.1.** *Let  $\lambda \in K$ , let  $\ell_i = \lambda^{q^{i-1}}$  for  $1 \leq i \leq d'$ , and let  $\ell_{ij} = \ell_i \ell_j$  for  $1 \leq i \leq j \leq d'$ . Suppose that the order of  $\lambda$  is divisible by a primitive prime divisor  $r$  of  $q^{d'} - 1$ , and suppose for some integer  $t$ , not divisible by  $r$ , we have  $\ell_{ij}^t = 1$ . Then  $d'$  is even, and  $j - i = d'/2$ .*

*Proof.* If  $\ell_{ij}^t = 1$  then  $1 = \lambda^{t(q^{i-1} + q^{j-1})} = \lambda^{tq^{i-1}(1+q^{j-i})}$ , so  $r$  divides  $tq^{i-1}(1+q^{j-i})$ . Since  $r$  does not divide  $q$  or  $t$ , and  $r$  is prime, it follows that  $r \mid (1 + q^{j-i})$ , and so  $r$  divides  $q^{2(j-i)} - 1$ . Since  $r$  is a primitive prime divisor of  $q^{d'} - 1$ , it follows that  $d' \mid 2(j-i)$ , and since  $0 < j-i < d'$ , we have  $0 < 2(j-i) < 2d'$  and so  $2(j-i) = d'$ .  $\square$

Lemma 5.1, with  $t = 1$ , is crucial in determining when a special element  $s$  has an eigenvalue 1. Note that Lemma 5.1 provides only a necessary condition, and not a sufficient condition: in some cases, the eigenvalue  $\ell_{1,d'/2+1}$  may be different from 1 (this is dependent on the order of  $\lambda$ ).

The existence of a fixed-point space of  $s$  in its action on  $(V \otimes V)_K$  may seem unfortunate (in the sense that it guarantees that not all of the eigenspaces can be 1-dimensional). However, in Section 2 we observe that, in all but the Unitary and Linear cases,  $G$  has fixed points in its action on  $M(V) \cong V \otimes V$ , and so these products equalling 1 is inevitable – we cannot hope to find an element in  $G$  with no fixed points.

We now address coincidences among the  $\ell_{ij}$  other than those corresponding to fixed points: we seek pairs  $(i, j), (m, n)$  such that  $\ell_{ij} = \ell_{mn}$ . We begin by exploiting the symmetry of the problem under the action of  $\sigma$  as much as we can.

**Lemma 5.2.** *Suppose  $q$  is a prime power, and  $d'$  an even integer with  $d' \geq 6$ . Let  $K = \mathbb{F}_{q^{d'}}$ , let  $\lambda \in K$ , and suppose that  $o(\lambda)$  is divisible by a primitive prime divisor  $r$  of  $q^{d'} - 1$ . Let  $\ell_i = \lambda^{q^{i-1}}$ , for  $1 \leq i \leq d'$ , and let  $\ell_{ij} = \ell_i \ell_j$  for  $1 \leq i, j \leq d'$ . Suppose that there exist integers  $i, j, m, n \in \{1, \dots, d'\}$ , satisfying*

$$\ell_{ij} = \ell_{mn}.$$

*Then at least one of the following holds:*

- (i)  $\{i, j\} = \{m, n\}$ ;
- (ii)  $d'$  is even, and  $\text{res}_{d'}(j-i) = \text{res}_{d'}(n-m) = d'/2$ ;
- (iii) There exist integers  $k, s, t, \alpha$ , with  $1 \leq k \leq d'/2$ , and  $1 \leq s < t \leq d'$ , such that  $\ell_{1k} = \ell_{st}$ , and  $\ell_{ij} = \ell_{1k}^{q^\alpha}$ .

*Proof.* Suppose that  $\text{res}_{d'}(j-i) = \text{res}_{d'}(n-m)$ . Then setting  $t' = \text{res}_{d'}(i-m)$ , we have  $\text{res}_{d'}(m+t') = i$ , and  $\text{res}_{d'}(n+t') = \text{res}_{d'}(n-m+i) = \text{res}_{d'}(j-i+i) = j$ , and so

$$\ell_{mn}^{q^{t'}} = \ell_{m+t', n+t'} = \ell_{ij} = \ell_{mn}.$$

Thus  $\ell_{mn}^{q^{t'}-1} = 1$ . If  $t' = d'$  then  $m = i, j = n$  and we are in case (i). Assume  $t' < d'$ : then since  $r$  is a primitive prime divisor of  $q^{d'} - 1$ ,  $r$  does not divide  $q^{t'} - 1$ . Then by Lemma 5.1 (with  $t = q^{t'} - 1$ ), we have  $\text{res}_{d'}(n-m) = \text{res}_{d'}(j-i) = d'/2$ .

Suppose, then, that  $\text{res}_{d'}(j-i) \neq \text{res}_{d'}(n-m)$  and so at least one of  $\text{res}_{d'}(j-i), \text{res}_{d'}(n-m)$  is distinct from  $d'/2$ , and at least one is distinct from  $d'$ . If  $\text{res}_{d'}(j-i) = d'/2$ , or if  $\text{res}_{d'}(n-m) = d'$  then we switch  $\{i, j\}$  with  $\{m, n\}$ : then we may assume that  $\text{res}_{d'}(n-m) \neq d'$  and  $\text{res}_{d'}(j-i) \neq d'/2$ .

If  $\text{res}_{d'}(j-i) < d'/2$ , then setting  $k = \text{res}_{d'}(j-i+1)$ , and  $\alpha = \text{res}_{d'}(i-1)$ , we have  $\ell_{ij}^{q^{d'-\alpha}} = \ell_{ij}^{q^{-i+1}} = \ell_{1, j-i+1} = \ell_{1k}$ . Set  $\{s, t\} = \{\text{res}_{d'}(m-i+1), \text{res}_{d'}(n-i+1)\}$ , with  $s, t$  ordered so that  $s < t$ . Note that since  $\text{res}_{d'}(n-m) \neq d'$  we have  $m \neq n$ , implying that  $s \neq t$ . Then  $\ell_{ij} = \ell_{1k}^\alpha$ ,

$$\ell_{1k} = \ell_{mn}^{q^{d'-\alpha}} = \ell_{mn}^{q^{-i+1}} = \ell_{m-i+1, n-i+1} = \ell_{st},$$

and  $k = \text{res}_{d'}(j-i+1) < d'/2 + 1$ , and so  $k \leq d'/2$  as required.

On the other hand, if  $\text{res}_{d'}(j-i) > d'/2$ , then  $\text{res}_{d'}(i-j) < d'/2$ . Then setting  $k = \text{res}_{d'}(i-j)+1$ , and  $\alpha = \text{res}_{d'}(j-1)$ , we have  $\ell_{ij}^{q^{d'-\alpha}} = \ell_{ij}^{q^{-j+1}} = \ell_{i-j+1, 1} = \ell_{1k}$ . Set  $\{s, t\} = \{\text{res}_{d'}(m-j+1), \text{res}_{d'}(n-j+1)\}$  with  $s, t$  again ordered so that  $s < t$ . Then we have  $\ell_{ij} = \ell_{1k}^\alpha$ ,  $\ell_{1k} = \ell_{st}$ , and again  $k \leq d'/2$  as required.  $\square$

The upshot of Lemma 5.2 is that in our search for coincidences  $\ell_{ij} = \ell_{mn}$  among our eigenvalues, we may assume without loss of generality that  $i = 1, j \leq d'/2$  and  $m \neq n$ . The first case we deal with is the Linear Case, where the order of  $\lambda$  is largest:

**Lemma 5.3.** *Suppose  $q$  is a prime power, and  $d'$  an integer with  $d' \geq 4$ . Let  $\lambda \in K$  have order a multiple of  $\frac{q^{d'}-1}{q-1}$ . Let  $\ell_i = \lambda^{q^{i-1}}$ , for  $1 \leq i \leq d'$ , and let  $\ell_{ij} = \ell_i \ell_j$  for  $1 \leq i \leq j \leq d'$ . Suppose there exist integers  $j, m, n$  such that  $\ell_{1j} = \ell_{mn}$ , with  $1 \leq j \leq d'/2$  and  $1 \leq m < n \leq d'$ , with  $j \neq 1$  if  $q$  is even. Then  $(1, j) = (m, n)$ .*

*Proof.* If  $\ell_{1j} = \ell_{mn}$  then  $\lambda^{1+q^{j-1}-q^{m-1}-q^{n-1}} = 1$ , and hence

$$1 + q^{j-1} - q^{m-1} - q^{n-1} \equiv 0 \pmod{\frac{q^d-1}{q-1}}.$$

This is a solution of equation (1), and the result then follows from Proposition 4.1.  $\square$

In all other cases things are more difficult, and most of Section 4 is devoted to aspects of the proof that the  $\ell_{ij}$  rarely coincide.

**Lemma 5.4.** *Suppose  $q$  is a prime power, and  $d'$  an integer with  $d' \geq 6$ . Let  $\lambda \in K$  have order  $q^{d'/2} + 1$ . Let  $\ell_i = \lambda^{q^{i-1}}$ , for  $1 \leq i \leq d'$ , and let  $\ell_{ij} = \ell_i \ell_j$  for  $1 \leq i \leq j \leq d'$ . Suppose there exist integers  $j, m, n$  such that  $\ell_{1j} = \ell_{mn}$ , with*

$1 \leq j \leq d'/2$  and  $1 \leq m < n \leq d'$ , with  $j \neq 1$  if  $q$  is even. Then one of the following holds:

- (i)  $\{1, j\} = \{m, n\}$  (the trivial coincidence);
- (ii)  $q = 2, j = d'/2 - 1, m = d' - 1, n = d$ ;
- (iii)  $q = 2, j = 2, m = d'/2$ , and  $n = 3$ ;
- (iv)  $q = 3, j = 1, m = 2$ , and  $n = d'/2 + 1$ .

*Proof.* Solutions to  $\ell_{1j} = \ell_{mn}$  are integer solutions to the equation

$$1 + q^{j-1} - q^{m-1} - q^{n-1} \equiv 0 \pmod{o(\lambda)},$$

for  $1 \leq j \leq d'/2$ , and  $1 \leq m \leq n \leq d'$ . Now if  $m > d'/2$ , then

$$q^{m-1} = q^{m-d'/2-1}(q^{d'/2} + 1) - q^{m-d'/2-1},$$

and so

$$q^{m-1} \equiv -q^{m-d'/2-1} \pmod{q^{d'/2} + 1}.$$

The same argument holds if  $n > d'/2$ , and so we have

$$1 + q^{j-1} + \epsilon_m q^{m'-1} + \epsilon_n q^{n'-1} \equiv 0 \pmod{q^{d'/2} + 1},$$

where

$$m' = \begin{cases} m & \text{when } m \leq d'/2 \\ m - d'/2 & \text{when } m > d'/2, \end{cases} \quad \text{and} \quad \epsilon_m = \begin{cases} -1 & \text{when } m \leq d'/2 \\ +1 & \text{when } m > d'/2, \end{cases}$$

and  $n', \epsilon_n$  are defined likewise. Note that while  $m'$  may be equal to  $n'$ , since  $m < n$ , we have  $(\epsilon_m, m') \neq (\epsilon_n, n')$ , and all of  $j, m', n'$  lie between 1 and  $d'/2$ . That is,  $(j, m', \epsilon_m, n', \epsilon_n)$  is a set of solutions to equation

$$1 + q^{j-1} + \epsilon_m q^{m'-1} + \epsilon_n q^{n'-1} \equiv 0 \pmod{q^{d'/2} + 1}.$$

This is precisely (3) in Section 4, and the result follows by Proposition 4.3.  $\square$

Note here that the solutions (ii), (iii) in Lemma 5.4 are essentially ‘the same’ coincidence: one can be obtained from the other by switching  $(1, j)$  with  $(m, n)$  and cycling under the action of  $\sigma$ . We now address the Unitary case: note here that  $d'$  is always odd (see Table 2), and so  $d'/2$  is not an integer. Thus when Lemma 5.2 allows us to assume that  $j \leq d'/2$ , we may strengthen this to assume that  $j \leq (d' - 1)/2$ .

**Lemma 5.5.** *Suppose  $q$  is square a prime power, and  $d'$  an odd integer with  $d' \geq 3$ .*

*Let  $\lambda \in K$  have order  $\frac{\sqrt{q^{d'}+1}}{\sqrt{q}+1}$ . Let  $\ell_i = \lambda^{q^{i-1}}$ , for  $1 \leq i \leq d'$ , and let  $\ell_{ij} = \ell_i \ell_j$  for  $1 \leq i \leq j \leq d'$ . Suppose there exist integers  $j, m, n$  such that  $\ell_{1j} = \ell_{mn}$ , with  $1 \leq j \leq (d' - 1)/2$  and  $1 \leq m < n \leq d'$ , with  $j \neq 1$  if  $q$  is even. Then  $(1, j) = (m, n)$ .*

*Proof.* Define  $\epsilon_m, m', \epsilon_n, n'$  as in the proof of Lemma 5.4 above: then by an identical argument, since  $o(\lambda) \mid (q^{d'/2} + 1)$  (where  $q^{d'/2}$  denotes  $\sqrt{q^{d'}}$ ), we have that  $q^{m-1} \equiv \epsilon_m q^{m'-1}$  modulo  $o(\lambda)$ , and so a solution to  $\ell_{1j} = \ell_{mn}$  corresponds to a solution to

$$1 + q^{j-1} + \epsilon_m q^{m'-1} + \epsilon_n q^{n'-1} \equiv 0 \pmod{\frac{\sqrt{q^{d'}+1}}{\sqrt{q}+1}}.$$

This is precisely equation (5) in Proposition 4.4, and the result follows.  $\square$

We now address the possibility of coincidence which are specific to the cases  $d' = d - 2, d - 1$ .

**Lemma 5.6.** *Suppose  $q$  is a prime power, and  $d'$  an even integer with  $d'/2 \geq 3$ . Let  $K = \mathbb{F}_{q^{d'}}$ , let  $\lambda \in K$ , and let  $\mu \in K$  have order  $q + 1$ . Let  $\ell_i = \lambda^{q^{i-1}}$ , for  $1 \leq i \leq d'$ , let  $m_1 = \mu, m_2 = \mu^q$ , and let  $\ell_{ij} = \ell_i \ell_j$  for  $1 \leq i, j \leq d'$ . Suppose that there exist integers  $i, j, k \in \{1, \dots, d'\}$ , and  $t \in \{1, 2\}$ , satisfying*

$$\ell_{ij} = \ell_k m_t.$$

*Then there exist integers  $r, s, n, \alpha$ , with  $1 \leq r \leq d'/2, 1 \leq s \leq d', 1 \leq n \leq 2$ , such that  $\ell_{1r} = \ell_s m_n$ , and  $\ell_{ij} = \ell_{1r}^{q^\alpha}$ .*

*Proof.* Set  $r = \min\{\text{res}_{d'}(j - i + 1), \text{res}_{d'}(i - j + 1)\}$ : if  $r = \text{res}_{d'}(j - i + 1)$ , then we have  $\ell_{1k}^{q^{i-1}} = \ell_{1+i-1, k+i-1} = \ell_{ij}$ , and so setting  $\alpha = d' - i + 1$ , we have that  $\ell_{1k} = \ell_{ij}^{q^\alpha}$ , and

$$\ell_{1k} = \ell_{ij}^{q^\alpha} = (\ell_k m_t)^{q^\alpha} = \ell_{\text{res}_{d'}(k+\alpha)} m_{\text{res}_2(t+\alpha)}.$$

Then setting  $s = \text{res}_{d'}(k + \alpha), n = \text{res}_2(t + \alpha)$ , the result holds. When  $r = \text{res}_{d'}(i - j + 1)$ , the result holds by an identical argument, with  $\alpha = d' - j + 1$ .  $\square$

**Lemma 5.7.** *Suppose  $q$  is a prime power, and  $d'$  an even integer with  $d'/2 \geq 3$ . Let  $\lambda \in K$  have order  $q^{d'/2} + 1$ , and let  $\mu \in K$  have order  $q + 1$ . Let  $\ell_i = \lambda^{q^{i-1}}$ , for  $1 \leq i \leq d'$ , let  $m_i = \mu^{q^{i-1}}$  for  $1 \leq i \leq 2$ , and let  $\ell_{ij} = \ell_i \ell_j$  for  $1 \leq i \leq j \leq d'$ . Suppose there exist integers  $j, s, t$  such that  $\ell_{1j} = \ell_s m_t$ , with  $1 \leq j, s \leq d'$  and  $1 \leq t \leq 2$ , with  $j \neq 1$  if  $q$  is even. Then  $q = 2$ , and one of the following holds:*

- (i)  $d' = 10, j = 3, \epsilon_m = -1, m' = 5$ ;
- (ii)  $j = 1, \epsilon_m = -1, m' = 2$ ; or
- (iii)  $d' = 10, \epsilon_m = 1, \{j, m'\} = \{2, 4\}$ .

*Proof.* Since  $o(\mu) = q + 1$ , we have that  $\ell_{1j}^{q+1} = (\ell_s m_t)^{q+1} = \ell_s^{q+1}$ , and so  $\lambda^{(1+q^{j-1})(q+1)} = \lambda^{q^{s-1}(q+1)}$ : that is,

$$(1 + q^{j-1} - q^{s-1})(q + 1) \equiv 0 \pmod{q^{d'/2} + 1}.$$

As in the proof of Lemma 5.4, set

$$s' = \begin{cases} s & \text{when } s \leq d'/2 \\ s - d'/2 & \text{when } s > d'/2, \end{cases} \quad \text{and} \quad \epsilon_s = \begin{cases} -1 & \text{when } s \leq d'/2 \\ +1 & \text{when } s > d'/2, \end{cases}$$

and we have that  $\epsilon_s q^{s'-1} \equiv -q^{s-1}$  modulo  $q^{d'/2} + 1$ , implying

$$(1 + q^{j-1} + \epsilon_s q^{s'-1})(1 + q) \equiv 0 \pmod{q^{d'/2} + 1}.$$

This is precisely equation (6), and the result follows by Proposition 4.5.  $\square$

**Lemma 5.8.** *Suppose  $q$  is a prime power, and  $d'$  an even integer with  $d'/2 \geq 3$ . Let  $K = \mathbb{F}_{q^{d'}}$ , and let  $\lambda \in K$ . Let  $\ell_i = \lambda^{q^{i-1}}$ , for  $1 \leq i \leq d'$ , let  $m_1 = \mu, m_2 = \mu^q$ , and let  $\ell_{ij} = \ell_i \ell_j$  for  $1 \leq i, j \leq d'$ . Suppose that there exist integers  $i, j, k \in \{1, \dots, d'\}$ , satisfying*

$$\ell_{ij} = \ell_k.$$

*Then there exist integers  $r, s, \alpha$ , with  $1 \leq r \leq d'/2, 1 \leq s \leq d'$ , such that  $\ell_{1r} = \ell_s$ , and  $\ell_{ij} = \ell_{1r}^{q^\alpha}$ .*

*Proof.* This follows immediately by the same proof as Lemma 5.6, replacing  $\mu$  with 1.  $\square$

**Lemma 5.9.** *Suppose  $q$  is a prime power, and that  $d'$  is an even integer with  $d' \geq 6$ . Suppose that  $\lambda \in K$  has order  $q^{d'/2} + 1$ , let  $\ell_i = \lambda^{q^{i-1}}$  for  $1 \leq i \leq d'$ , and let  $\ell_{ij} = \ell_i \ell_j$ .*

*Suppose there exist integers  $j, s, t$  such that  $\ell_{1j} = \ell_s$ , with  $1 \leq j \leq d'/2, 1 \leq s \leq d'$ , with  $j \neq 1$  if  $q$  is even. Then  $q = 2, j = 1, \epsilon_m = -1, m' = 2$ .*

*Proof.* By an identical argument to the proof of Lemma 5.7 above (without raising to the  $(q+1)$ st power), we have that

$$1 + q^{j-1} + \epsilon_s q^{s'-1} \equiv 0 \pmod{q^{d'/2} + 1}$$

where  $s', \epsilon_s$  are as defined in the proof of Lemma 5.7. Then  $j, \epsilon_s, s', q, d'$  are solutions to the equation (7) in Section 4. Then the result follows from Corollary 4.6.  $\square$

Once again we must treat the Unitary case separately.

**Lemma 5.10.** *Suppose  $q$  is a square prime power, and that  $d'$  is an odd integer with  $d' \geq 3$ . Suppose that  $\lambda \in K$  has order a multiple of  $\frac{\sqrt{q^{d'}+1}}{\sqrt{q}+1}$ , let  $\ell_i = \lambda^{q^{i-1}}$  for  $1 \leq i \leq d'$ , and let  $\ell_{ij} = \ell_i \ell_j$ .*

*Then there do not exist integers  $j, s, t$  such that  $\ell_{1j} = \ell_s$ , with  $1 \leq j \leq (d'-1)/2, 1 \leq s \leq d'$ .*

*Proof.* Again by an identical argument to the proof of Lemma 5.7, we have that

$$1 + q^{j-1} + \epsilon_s q^{s'-1} \equiv 0 \pmod{\frac{\sqrt{q^{d'}+1}}{\sqrt{q}+1}}$$

where  $s', \epsilon_s$  are as defined in the proof of Lemma 5.7. Then  $j, \epsilon_s, s', q, d'$  are solutions to the equation (8) in Section 4. Then the result follows from Corollary 4.7.  $\square$

**Lemma 5.11.** *Let  $G$  be a classical group as in one of the lines of Table 2, and let  $s \in G$  be a special element as defined in Definition 3.3, with eigenvalues  $\{\ell_i \mid 1 \leq i \leq d\}$  as in Lemma 3.6, and let  $\mathcal{E}(s, V) = \{e_i \mid 1 \leq i \leq d\}$  be as defined in Lemma 3.6. Suppose that in the Linear and Unitary cases, we have  $d \geq 4$ ; in the remaining cases with  $d' = d$  we have  $d' \geq 6$ ; in the cases  $d' = d-1, d-2$  we have  $d' \geq 8$ . Then the eigenvalues of  $s$  in its action on  $(V \otimes V)_K$  are*

$$\{\ell_{ij} := \ell_i \ell_j \mid 1 \leq i \leq j \leq d\},$$

*and the following hold:*

- (i) *if  $\ell_{ij} = 1$  then either  $d' = d-1$  and  $i = j = d$ ; or  $d' = d-2$  and  $\{i, j\} = \{d-1, d\}$ ; or  $i \leq d', j \leq d', \text{res}_{d'}(j-i) = d'/2$ , and  $G$  is Symplectic or Orthogonal;*
- (ii) *for each pair  $(i, j)$  with  $1 \leq i \leq j \leq d$ , the  $\ell_{ij}$ -eigenspace of  $s$  in its action on  $(V \otimes V)_K$  contains the tensor products  $e_i \otimes e_j, e_j \otimes e_i$ ; and*
- (iii) *the  $\ell_{ij}$ -eigenspace of  $s$  in its action on  $(V \otimes V)_K$  is precisely  $\langle e_i \otimes e_j, e_j \otimes e_i \rangle$ , except when  $\ell_{ij} = 1$  and  $G \in \{\text{Sp}(d, q), \text{SO}^\epsilon(d, q)\}$ ; or when  $G \in \{\text{Sp}(d, 3), \text{SO}^\epsilon(d, 3)\}$ , and  $\text{res}_{d'}(j-i) \in \{d', d'/2+1\}$ ; or when  $G \in \{\text{Sp}(d, 2), \text{SO}^\epsilon(d, 2)\}$  and  $\text{res}_{d'}(j-i) \in \{1, d'/2-2\}$ .*



*Proof.* By Lemma 5.1, if  $\ell_{ij} = 1$  and  $1 \leq i \leq j \leq d'$  then  $d'$  is even and  $\text{res}_{d'}(j-i) = d'/2$ . Since (when  $d' = d - 2$ ) for  $\mu \in K$  of order  $q + 1$  we have that  $\mu^2 \neq 1$ , the only other possible pairs giving  $\ell_{ij} = 1$  are those listed. In the Linear case we have that  $o(s) > \frac{q^d - 1}{q - 1}$ , and so  $\ell_{1, d'/2+1} = \lambda^{q^{d'/2+1}} \neq 1$ , and so 1 is not an eigenvalue. In the Unitary case, we have that  $d'$  is odd, and so  $\ell_{ij} = 1$  only if  $i = j = d$ , and so in this case the eigenspace of 1 is precisely  $\langle e_d \otimes e_d \rangle$ . In all other cases when  $\ell_{ij} = 1$ , the eigenspace of 1 has dimension greater than 1. Thus (i) is proved. (ii) follows from Lemma 2.1; and (iii) follows from (i), and from Lemma 5.2 and Lemma 5.3 in the Linear case; Lemma 5.2 and Lemmas 5.4, 5.5 in non-Linear cases with  $d' = d$ ; Lemma 5.8 and Lemmas 5.9, 5.10 when  $d' = d - 1$ ; and Lemma 5.6 and Lemma 5.7 when  $d' = d - 2$ .  $\square$

Having completely described the action of a special element on  $(V \otimes V)_K$ , we turn to the submodule  $S^2(V)$ . The eigenstructure of a special element's action on  $S^2(V)_K$  and can be 'read' directly from Lemma 5.11 using Lemma 2.1: in the next section, we provide concrete links between the action of an arbitrary  $g \in G$  on various bases for  $S^2(V)_K$  (and hence its irreducible constituents).

## 6. THE ACTION OF A SPECIAL ELEMENT ON THE SYMMETRIC SQUARE $S^2(V)_K$

**Lemma 6.1.** *Let  $G$  be a Classical Group as in one of the lines of Table 2, and let  $s \in G$  be a special element as defined in Definition 3.3, with eigenvalues  $\{\ell_i \mid 1 \leq i \leq d\}$  as in Lemma 3.6, and let  $\mathcal{E}(s, V) = \{e_i \mid 1 \leq i \leq d\}$  be as defined in Lemma 3.6.*

Define

$$\mathcal{E}(s, S^2(V)) = \{e_{s, S^2(V), ij} \mid 1 \leq i \leq j \leq d\},$$

where

$$e_{s, S^2(V), ij} = e_i \otimes e_j + (1 - \delta_{ij})e_j \otimes e_i.$$

Suppose that in the Linear and Unitary cases, we have  $d \geq 4$ ; in the remaining cases with  $d' = d$  we have  $d' \geq 6$ ; and in the remaining cases with  $d' = d - 1, d - 2$  we have  $d' \geq 8$ . Then the eigenvalues of  $s$  in its action on  $S^2(V)_K$  are

$$\{\ell_{ij} := \ell_i \ell_j \mid 1 \leq i \leq j \leq d\},$$

and the following hold:

- (i) if  $\ell_{ij} = 1$  then  $i \leq d', j \leq d'$  and the condition in the 5th column of the appropriate line of Table 2 holds;
- (ii) for each pair  $(i, j)$ , the  $\ell_{ij}$ -eigenspace of  $s$  contains  $e_{s, S^2(V), ij}$ ; and
- (iii) the  $\ell_{ij}$ -eigenspace of  $s$  is precisely  $\langle e_{s, S^2(V), ij} \rangle$ , except when either  $\ell_{ij} = 1$  and  $G \in \{\text{Sp}(d, q), \text{SO}^\epsilon(d, q)\}$ ; or  $G \in \{\text{Sp}(d, 3), \text{SO}^\epsilon(d, 3)\}$ .

*Proof.* This follows immediately from Lemma 5.11 and 2.1 (note that the exceptional cases in Lemma 5.11 for  $q = 2$  do not apply here as  $q$  is odd).  $\square$

**Lemma 6.2.** *Let  $G$  be a classical group, let  $W$  be an  $FG$ -module isomorphic to  $S^2(V)$ , and let  $\text{App}_W$  be the set of pairs  $(i, j)$  of integers such that, for any special element  $s \in G$ , the  $\ell_{ij}$ -eigenspace of  $s$  in its action on  $W$  has dimension 1. Then:*

- (i) if  $G \in \{\text{SL}(d, q), \text{SU}(d, q)\}$ , then  $d' = d$  and  $\text{App}_W = \{(i, j) \mid 1 \leq i \leq j \leq d\}$ ;

- (ii) if  $G \in \{\mathrm{Sp}(d, q), \mathrm{SO}^-(d, q)\}, q \geq 5$ , then  $d' = d$  and  $(i, j) \in \mathrm{App}_W$  if and only if  $1 \leq i \leq j \leq d$ , and  $j - i \neq d/2$ ;
- (iii) if  $G \in \{\mathrm{SO}^\circ(d, q) \text{ for } d \text{ odd}\}, q \geq 5$ , then  $d' = d - 1$  and  $(i, j) \in \mathrm{App}_W$  if and only if either  $1 \leq i \leq j \leq d'$ , and  $j - i \neq d'/2$ ; or  $1 \leq i \leq d'$  and  $j = d$ ;
- (iv) if  $G = \mathrm{SO}^+(d, q), q \geq 5$ , then  $d' = d - 2$  and  $(i, j) \in \mathrm{App}_W$  if and only if either  $1 \leq i \leq j \leq d'$ , and  $j - i \neq d'/2$ ; or  $1 \leq i \leq d'$  and  $d' < j \leq d$ ; or  $d' < i \leq d$  and  $j = i$ .

Note that in all cases, if  $1 \leq i \leq j \leq d', j - i \neq d'/2$ , we have  $(i, j) \in \mathrm{App}_W$ .

*Proof.* This follows immediately from Lemma 6.1. Note that while the eigenvalues and eigenvectors depend upon  $s$ , the set of pairs  $(i, j) \in \mathrm{App}_W$  does not.  $\square$

While the notation  $e_{s, S^2(V), ij}$  is cumbersome, there are very many modules and bases to consider, and it is sometimes needed for clarity. We will often simply write  $e_{ij}$  when there is no ambiguity.

**Definition 6.3.** Let  $G$  be a classical group as in one of the lines of Table 2, let  $s \in G$  be a special element as in Definition 3.3, and for  $1 \leq i \leq j \leq d$ , let  $e_{ij} := e_{s, S^2(V), ij}$  be as defined in Lemma 6.1. Let  $\sigma$  be the Frobenius automorphism of the extension  $K/F$ .

Suppose that  $\mathcal{F} = \{f_{ij} \mid 1 \leq i \leq j \leq d\}$  is a basis for  $S^2(V)_K$ . Then  $\mathcal{F}$  is said to satisfy the  $\sigma$ -relations for  $S^2(V)$  if the following hold:

- (i) for  $1 \leq i \leq j \leq d' - 1$ ,  $f_{ij}^\sigma = f_{i+1, j+1}$ ;
- (ii) for  $1 \leq i \leq d' - 1$ ,  $f_{id'}^\sigma = f_{1, i+1}$ , and  $f_{d'd'}^\sigma = f_{11}$ ;
- (iii) if  $d' = d - 1$  then, for  $1 \leq i \leq d'$ ,  $f_{i, d}^\sigma = f_{i+1, d}$ , and  $f_{dd}^\sigma = f_{dd}$ ;
- (iv) if  $d' = d - 2$  then, for  $1 \leq i \leq d'$ ,  $f_{i, d-1}^\sigma = f_{\mathrm{res}_{d'}(i+1), d}$ ,  $f_{i, d}^\sigma = f_{\mathrm{res}_{d'}(i+1), d-1}$ , and  $f_{d-1, d-1}^\sigma = f_{dd}$ ,  $f_{d-1, d}^\sigma = f_{d-1, d}$ , and  $f_{dd}^\sigma = f_{d-1, d-1}$ .

If  $\mathcal{F}$  has a partial labelling  $\{f_{ij} \mid (i, j) \in \mathrm{App}_W\} \subset \mathcal{F}$ , then we say that  $\mathcal{F}$  satisfies the  $\sigma$ -relations for  $\mathrm{App}_W$  if the relations hold for all  $(i, j) \in \mathrm{App}_W$ .

**Lemma 6.4.** Let  $G$  be a classical group as in one of the lines of Table 2, let  $s \in G$  be a special element as defined in Definition 3.3, and let  $\mathcal{E}(s, S^2(V)) = \{e_{ij} := e_{s, S^2(V), ij} \mid 1 \leq i \leq j \leq d\}$  as defined in Lemma 6.1. Then  $\mathcal{E}(s, S^2(V))$  satisfies the  $\sigma$ -relations for  $S^2(V)$ .

*Proof.* The relations follow immediately from the fact that, by Lemma 3.6, the  $\sigma$ -relations for  $V$  (as in Definition 3.5) hold for  $\{e_i \mid 1 \leq i \leq d\}$ .  $\square$

**Lemma 6.5.** Let  $G$  be a classical group as in one of the lines of Table 2, let  $s \in G$  be a special element as defined in Definition 3.3, let  $W = S^2(V)$ , and let  $\mathcal{E} = \mathcal{E}(s, S^2(V)) = \{e_{ij} \mid 1 \leq i \leq j \leq d\}$  be as in Definition 6.3.

Suppose that there exists a basis  $\mathcal{F}_{S^2(V)} := \mathcal{F}(s, S^2(V), \mathcal{E}) := \{f_{ij} := f_{s, V, \mathcal{E}, ij} \mid 1 \leq i \leq j \leq d\}$  for  $W_K$  such that, for every pair  $(i, j)$  with  $1 \leq i \leq j \leq d$ , we have that  $f_{s, V, \mathcal{E}, ij} \in \langle e_{ij} \rangle$ , and  $\mathcal{F}_{S^2(V)}$  satisfies the  $\sigma$ -relations for  $S^2(V)$  as defined in Lemma 6.1.

Then there exists an extension field  $L$  of  $K$  of degree at most 2, a basis  $\mathcal{F}_V = \mathcal{F}(s, V, \mathcal{F}_{S^2(V)}) := \{f_i \mid 1 \leq i \leq d\}$  for  $V_L$ , and a set  $\mathcal{C} = \mathcal{C}(s, \mathcal{F}_{S^2(V)}, \mathcal{F}_V) :=$

$\{c_{ij} \mid 1 \leq i \leq j \leq d\} \subseteq L$ , such that  $\mathcal{F}_V$  satisfies the almost- $\sigma$ -relations for  $V$ , and for  $1 \leq i \leq j \leq d$ , we have

$$f_{ij} = c_{ij}(f_i \otimes f_j + (1 - \delta_{ij})f_j \otimes f_i).$$

Moreover, we have that  $c_{11} = 1$ ; and if  $d' < d$ , we have  $c_{1j} = 1$  for  $j > d'$ .

*Proof.* Let  $\mathcal{E}_V := \{e_i\}$  be as defined in Lemma 3.6. Then since each  $f_{ij}$  is a scalar multiple of  $e_{ij}$ , there exist constants  $c'_{ij} \in K$  such that  $f_{ij} = c'_{ij}e_{ij}$ . Suppose that for every  $i$ , we set  $f_i = a_i e_i$ , for  $a_i \in L$ . Then for every  $i, j$ , we have that  $f_i \otimes f_j = (a_i e_i) \otimes (a_j e_j) = a_i a_j (e_i \otimes e_j)$ , and so

$$f_i \otimes f_j + (1 - \delta_{ij})f_j \otimes f_i = a_i a_j (e_i \otimes e_j + (1 - \delta_{ij})e_j \otimes e_i) = a_i a_j e_{ij}.$$

For  $1 \leq i \leq j \leq d'$ , set  $c_{ij} := c'_{ij}(a_i a_j)^{-1} \in L$ : then

$$c_{ij}(f_i \otimes f_j + (1 - \delta_{ij})f_j \otimes f_i) = c'_{ij}e_{ij} = f_{ij}.$$

This holds for all choices of  $\{a_i\}$ , and so we have a great deal of freedom. By [12, Theorem 2.14], we may choose a square root  $x$  of  $c'_{11}$  in the extension field  $L/K$ .

For  $1 \leq i \leq d'$ , set  $a_i = x^{q^{i-1}}$ : then  $a_1^2 = x^2 = c'_{11}$ , and so  $c_{11} = c'_{11}a_1^{-2} = 1$ , and when  $i < d'$ , we have  $f_i^\sigma = (a_i e_i)^\sigma = (x^{q^{i-1}})^q e_{i+1} = a_{i+1} e_{i+1} = f_{i+1}$ . When  $i = d$ , we have that  $e_d^\sigma = e_1$ , and so  $f_i^\sigma = a_d^q f_1 \in \langle f_1 \rangle$ , and so the almost- $\sigma$ -relations hold for  $i < d'$ . The other relations follow in a similar way.

If  $d' < d$ , then for  $j > d'$ , set  $a_j = c'_{1j}a_1^{-1}$ : then  $a_1 a_j = c'_{1j}$ , and we have  $c_{1j} = c_{1j}(a_1 a_j)^{-1} = 1$  as required.  $\square$

The purpose of Lemma 6.5 is to allow a safe ‘transition’ between an action of  $g \in G$  on  $S^2(V)_K$  to an action on  $V_L$  (although we will later show that this action remains within the confines of  $V_K$ ). However, it depends on our ability to find the constants  $c_{ij}$ , and this is not necessarily possible. There is, at one point in the procedure, a square root to be taken, and so a choice must be made, and a sign ambiguity introduced. The following result permits us to choose either path without regret.

**Lemma 6.6.** *Let  $G$  be a classical group as in one of the lines of Table 2, let  $s \in G$  be a special element as defined in Definition 3.3, let  $W = S^2(V)$ , and let  $\mathcal{E}_{S^2(V)} = \{e_{ij} \mid 1 \leq i \leq j \leq d\}$  be as defined in Lemma 6.1.*

*Suppose that there exists  $\mathcal{F}_{S^2(V)} := \{f_{s,V,\mathcal{E},ij} \mid 1 \leq i \leq j \leq d\}$ ,  $L, \mathcal{F}_V := \{f_i \mid 1 \leq i \leq d\}$ ,  $\mathcal{C}(s, \mathcal{F}_{S^2(V)}, \mathcal{F}_V) = \{c_{ij} \mid 1 \leq i \leq j \leq d\}$  as defined in Lemma 6.5.*

*Then define a basis  $\mathcal{F}_V^- := \{f_i^- \mid 1 \leq i \leq d\}$  and a set of constants  $\mathcal{C}^- = \mathcal{C}(s, \mathcal{F}_{S^2(V)}, \mathcal{F}_V)^- := \{c_{ij}^- \mid 1 \leq i \leq j \leq d\} \subset L$ , as follows:*

- (i) *for  $1 \leq i \leq d'$ , let  $f_i^- = (-1)^{i+1}f_i$ ; and for  $i > d'$  let  $f_i^- = f_i$ ; and*
- (ii) *for  $1 \leq i \leq j \leq d'$ , let  $c_{ij}^- := (-1)^{j-i}c_{ij}$ ; for  $1 \leq i \leq d'$ ,  $j > d'$ , let  $c_{ij}^- := (-1)^{i+1}c_{ij}$ ; and for all other  $(i, j)$  let  $c_{ij}^- := c_{ij}$ .*

*Then for  $1 \leq i \leq j \leq d$ , we have*

$$f_{ij} = c_{ij}^-(f_i^- \otimes f_j^- + (1 - \delta_{ij})f_j^- \otimes f_i^-).$$

*Proof.* Observe that, for  $1 \leq i \leq j \leq d'$ , we have

$$c_{ij}^-(f_i^- \otimes f_j^- + (1 - \delta_{ij})f_j^- \otimes f_i^-) = (-1)^{2j+2}c_{ij}(f_i \otimes f_j + (1 - \delta_{ij})f_j \otimes f_i),$$

and since  $2j + 2$  is even, this is precisely  $f_{ij}$ . When  $i \leq d', j > d'$ , we have

$$c_{ij}^-(f_i^- \otimes f_j^- + (1 - \delta_{ij})f_j^- \otimes f_i^-) = (-1)^{2(i+1)}c_{ij}(f_i \otimes f_j + (1 - \delta_{ij})f_j \otimes f_i),$$

which again is equal to  $f_{ij}$  since  $2(i+1)$  is even. If  $d' < i \leq j \leq d$  then the assertion holds trivially by the definitions.  $\square$

Lemma 6.6 allows us to ‘err’ in our search for the values of the  $c_{ij}$ , so long as we ‘accidentally’ find  $c_{ij}^-$ : in that case, **FindPreimage** will return the action of  $g \in G$  with respect to  $\mathcal{F}_V^-$  instead of  $\mathcal{F}_V$ , a mistake which is irrelevant to us, and by Lemma 6.5 above, is unavoidable. Note that we are only permitted to make *one* mistake: we must compute all of either  $\mathcal{C}$  or  $\mathcal{C}^-$ , and we cannot ‘mix and match’.

**Lemma 6.7.** *Let  $G$  be a classical group as in one of the lines of Table 2, let  $s \in G$  be a special element as defined in Definition 3.3, let  $W = S^2(V)$ . Let  $\mathcal{E}_{S^2(V)} = \{e_{ij} \mid 1 \leq i \leq j \leq d\}$  be as defined in Lemma 6.1, and let  $\mathcal{F}_V, \mathcal{C}$  be defined as in Lemma 6.5, and let  $\mathcal{F}_V^-, \mathcal{C}^-$  be as defined in Lemma 6.6.*

*Then for  $1 \leq i \leq j \leq d' - 1$ , we have  $c_{ij}^q = c_{i+1,j+1}$  and  $(c_{ij}^-)^q = c_{i+1,j+1}^-$ , and hence for  $1 \leq i \leq d'$ , we have  $c_{ii} = c_{ii}^- = 1$ .*

*Moreover, for every  $g \in G$ , and for all pairs  $(i, j), (k, \ell) \in \text{App}_W$ , we have the following, where  $\kappa_{ij,k\ell} := g_{f_{ij}f_{k\ell}}, a_{ij} = g_{f_i f_j}, a_{ij}^- = g_{f_i^- f_j^-}$ :*

(i) *The Basic Equations in the Symmetric Square Case hold for  $(\kappa_{ij,k\ell}), \mathcal{C}, (a_{ij}), \mathcal{C}^-, (a_{ij}^-)$ :*

$$(9) \quad \kappa_{ij,k\ell} = \frac{c_{ij}}{c_{k\ell}}(a_{ik}a_{j\ell} + (1 - \delta_{ij})a_{i\ell}a_{jk}) = \frac{c_{ij}^-}{c_{k\ell}^-}(a_{ik}^-a_{j\ell}^- + (1 - \delta_{ij})a_{i\ell}^-a_{jk}^-)$$

(ii) *for  $1 \leq i, j \leq d' - 1$ , we have  $a_{ij}^q = a_{i+1,j+1}$ ,  $(a_{ij}^-)^q = a_{i+1,j+1}^-$ .*

*Proof.* Since  $f_i^\sigma = f_{i+1}$  for all  $1 \leq i \leq d' - 1$ , and since  $\delta_{ij} = \delta_{i+1,j+1}$ , we have, for  $1 \leq i \leq j \leq d' - 1$ , that

$$\begin{aligned} f_{ij}^\sigma &= (c_{ij}(f_i \otimes f_j + (1 - \delta_{ij})f_j \otimes f_i))^\sigma \\ &= c_{ij}^q(f_{i+1} \otimes f_{j+1} + (1 - \delta_{i+1,j+1})f_{j+1} \otimes f_{i+1}) \\ &= c_{ij}^q(c_{i+1,j+1}^{-1}f_{i+1,j+1}), \end{aligned}$$

and so  $c_{ij}^q = c_{i+1,j+1}$  since, by definition, we have that  $f_{ij}^\sigma = f_{i+1,j+1}$ . Since, by Lemma 6.5,  $c_{11} = 1$ , we have that  $c_{ii} = 1$  for all  $i$ . The relations on  $c_{ij}^-$  follow immediately since  $c_{ij}^- = (-1)^{j-i}c_{ij}$ .

(i) follows immediately from Lemmas 2.3. For (ii), since  $f_i^\sigma = f_{i+1}$  for  $1 \leq i \leq d' - 1$ , and since  $f_i^\sigma \notin \langle f_2, \dots, f_{d'} \rangle$  for  $i \geq d'$ , we have that

$$f_i^{g\sigma} = \left( \sum_{j=1}^d a_{ij}f_j \right)^\sigma = \sum_{j=1}^{d'-1} a_{ij}^q f_{j+1} + v,$$

for some  $v \notin \langle f_2, \dots, f_{d'} \rangle$ . On the other hand

$$f_i^{\sigma g} = f_{i+1}^g = \sum_{j=1}^d a_{i+1,j} f_j = \sum_{j=0}^{d-1} a_{i+1,j+1} f_{j+1},$$

and so, since  $f_i^{g\sigma} = f_i^{\sigma g}$ , by equating coefficients of  $f_{j+1}$  for  $1 \leq j \leq d' - 1$ , we have  $a_{ij}^g = a_{i+1,j+1}$  as required. A similar argument shows that the relations hold among the  $a_{ij}^-$ , since  $(f_i^-)^{\sigma} = ((-1)^{i+1})^{\sigma} f_i^{\sigma} = (-1)^{i+1} f_{i+1} = -f_{i+1}$ .  $\square$

**Lemma 6.8.** *Let  $G$  be a Classical Group, let  $V$  be the natural  $FG$ -module, and let  $W$  be an  $FG$ -module such that  $W = (S^2(V)^*)^{\varphi}$ , where  $S^2(V)^*$  is an irreducible section of  $S^2(V)$  of codimension at most 2, and  $\varphi$  is an isomorphism of  $FG$ -modules, and let  $\nu$  be a homomorphism of  $FG$ -modules such that  $S^2(V)^* \leq S^2(V)^{\nu}$ .*

*Let  $s \in G$  be a special element, as in Definition 3.3, let  $\{\ell_{ij} \mid 1 \leq i \leq j \leq d'\}$  be the eigenvalues of  $s$  in  $S^2(V)_K$ , as in Lemma 6.1. Suppose that  $\mathcal{F}_W = \{f_{W,ij} \mid (i,j) \in \text{App}_W\} \cup \mathcal{F}'$  is a basis of  $W_K$  such that, for every  $(i,j) \in \text{App}_W$ , we have that  $f_{W,ij}$  is an  $\ell_{ij}$ -eigenvector for  $s$  in  $W_K$ , and  $\mathcal{F}_W$  satisfies the  $\sigma$ -relations for  $S^2(V)$  for all  $(i,j) \in \text{App}_W$  as in Definition 6.4.*

*Then there exists a basis  $\mathcal{F}_{S^2(V)} = \{\hat{f}_{ij} \mid 1 \leq i \leq j \leq d\}$  of  $S^2(V)_K$  such that  $\mathcal{F}_{S^2(V)}$  satisfies the  $\sigma$ -relations for  $S^2(V)$ , and for every  $(i,j) \in \text{App}_W$ , the following hold:*

- (i)  $\hat{f}_{ij}^{\nu} \in S^2(V)^*$ ;
- (ii)  $\hat{f}_{ij}^{\nu\varphi} = f_{ij}$ ; and
- (iii) for every  $g \in G$  and for all  $(i,j), (k,\ell) \in \text{App}_W$ , we have that  $g_{\hat{f}_{ij}\hat{f}_{k\ell}} = g_{f_{ij}f_{k\ell}}$ .

*Proof.* Note first that  $\nu$  is either the identity map, or the projection of  $S^2(V)$  onto a quotient by a subspace fixed pointwise by  $G$ . For each  $(1,j) \in \text{App}_W$ , choose a preimage of  $f_{1j}^{\varphi^{-1}}$  under  $\nu$ , and set  $\hat{f}_{1j}$  to be this preimage. Then for  $(i,j) \in \text{App}_W$  with  $2 \leq i \leq j \leq d'$ , set  $\hat{f}_{ij} := \hat{f}_{i-1,j-1}^{\sigma^{-1}}$ . If  $d' = d - 1$ , then for  $2 \leq i \leq d'$ , set  $\hat{f}_{id} := \hat{f}_{i-1,d}^{\sigma}$ . If  $d' = d - 2$ , then for  $2 \leq i \leq d'$ , set  $\hat{f}_{id} := \hat{f}_{i-1,d-1}^{\sigma}$ , and set  $\hat{f}_{i,d-1} := \hat{f}_{i-1,d}^{\sigma}$ . Choose a preimage of  $f_{d-1,d-1}^{\varphi^{-1}}$  under  $\nu$ , set  $\hat{f}_{d-1,d-1}$  to be this preimage, and set  $\hat{f}_{dd} = \hat{f}_{d-1,d-1}^{\sigma}$ . Then  $\hat{f}_{ij}$  has been defined for all pairs  $(i,j) \in \text{App}_W$ : for the remaining pairs with  $1 \leq i \leq j \leq d$ , choose  $\hat{f}_{ij}$  such that they satisfy the  $\sigma$ -relations for  $S^2(V)$ .

Now for all  $1 \leq i \leq j \leq d$ , we have that  $\hat{f}_{ij}$  is an  $\ell_{ij}$ -eigenvector for  $s$  in its action on  $S^2(V)$ , since the maps  $\nu, \varphi$  preserve eigenstructure, and since the action of  $\sigma$  maps  $\ell_{ij}$ -eigenvectors to  $\ell_{ij}^q$ -eigenvectors. By Lemma 6.1, for every  $(i,j) \in \text{App}_W$ , either  $G = \text{SU}(d, q)$ , or  $\ell_{ij} \neq 1$ . In the former case,  $\nu$  is the identity map, and so  $\hat{f}_{ij}^{\nu} \in S^2(V)^*$ . In the latter case,  $\hat{f}_{ij}$  is an  $\ell_{ij}$ -eigenvector for  $\ell_{ij} \neq 1$ , and so is not fixed by the action of  $s$ , and so since  $S^2(V)^*$  is the kernel of a linear form  $T$ , we have, by Lemma 2.2, that  $\hat{f}_{ij}^{\nu} \in S^2(V)^*$ .

Since  $\sigma$  commutes with  $\varphi, \nu$ , we have, for  $(i,j) \in \text{App}_W$  with  $2 \leq i \leq j \leq d'$ ,

that  $\hat{f}_{ij}^{\nu\varphi} = (\hat{f}_{i-1,j-1}^\sigma)^{\nu\varphi} = (\hat{f}_{i-1,j-1}^{\nu\varphi})^\sigma = f_{i-1,j-1}^\sigma = f_{ij}$ . By the same argument we have that  $\hat{f}_{ij}^{\nu\varphi} = f_{ij}$  for the remaining  $(i, j) \in \text{App}_W$ , and so (ii) holds. (iii) then follows.  $\square$

Lemma 6.8 ‘lifts’ us from a basis of  $W_K$  to a basis of  $S^2(V)_K$ : combining this with Lemma 6.7 ‘decomposes’ into one of two bases for  $V_L$  for which the Basic Equation holds whenever  $(i, j), (k, \ell) \in \text{App}_W$ . This set of equations is the tool for constructive recognition.

**Corollary 6.9.** *Let  $G$  be a Classical Group, let  $V$  be the natural  $FG$ -module, and let  $W$  be an  $FG$ -module such that  $W = (S^2(V)^*)^\varphi$ , where  $S^2(V)^*$  is an irreducible section of  $S^2(V)$  of codimension at most 2, and  $\varphi$  is an isomorphism of  $FG$ -modules.*

*Let  $s \in G$  be a special element, as in Definition 3.3, let  $\{\ell_{ij} \mid 1 \leq i \leq j \leq d'\}$  be the eigenvalues of  $s$  in  $S^2(V)_K$ , as in Lemma 6.1. Suppose that  $\mathcal{F}_W = \{f_{W,ij} \mid (i, j) \in \text{App}_W\} \cup \mathcal{F}'$  is a basis of  $W_K$  satisfying the conditions in Lemma 6.8.*

*Then there exists a field extension  $L$  of  $K$  of degree at most 2, a basis  $\mathcal{F}_V = \mathcal{F}(s, V, \mathcal{F}_W) = \{f_{V,i} \mid 1 \leq i \leq d\}$  of  $V_L$ , a set of constants  $\mathcal{C} = \{c_{ij} \mid (i, j) \in \text{App}_W\}$ , a basis  $\mathcal{F}_V^- = \{f_{V,i}^- \mid 1 \leq i \leq d\}$  and constants  $\mathcal{C}^- = \{c_{ij}^- \mid (i, j) \in \text{App}_W\}$  as defined in Lemma 6.6, such that, for every  $(i, j), (k, \ell) \in \text{App}_W$  and for every  $g \in G$ , the following hold, where  $\kappa_{ij,k\ell} = g_{f_{W,ij} f_{W,k\ell}}, a_{ij} = g_{f_{V,i} f_{V,j}}, a_{ij}^- = g_{f_{V,i}^- f_{V,j}^-}$ :*

- (i) *The Basic Equation (9) holds; and*
- (ii) *for  $1 \leq i, j \leq d' - 1$ , we have  $a_{ij}^q = a_{i+1,j+1}$ .*

*Moreover, we have  $c_{ii} = c_{ii}^- = 1$  for  $1 \leq i \leq d'$ , and if  $d' < d$ , we have  $c_{1j} = 1$  for  $d' < j \leq d$ .*

*Proof.* By Lemma 6.8, the basis  $\mathcal{F}_W$  gives rise to a basis  $\mathcal{F}$  of  $S^2(V)$  satisfying the conditions of Lemma 6.7: combining these two results, the result follows.  $\square$

## 7. THE ALGORITHM

In this Section we detail the steps in **Initialise** and **FindPreimage**. We first must find a Special Element  $s$  (by random search), and then find the eigenvalues of  $s$  in its action on  $W_K$ , a basis  $\mathcal{F}_W := \{f_{ij} \mid (i, j) \in \text{App}_W\} \cup \mathcal{F}'$  for  $W_K$  of  $s$ -eigenvectors, and constants  $c_{ij}$  for certain values of  $i, j$  satisfying the conditions of Lemma 6.8. Since  $S^2(V)$  contains the Alternating Square  $\wedge^2(V)$  when  $q$  is even (and so is irreducible in a nontrivial way) *we assume that  $q$  is odd*.

Parts of the procedure work for all odd  $q$ , but ultimately **Initialise** can be completed only when  $q \geq 5$  in certain cases (due to the exceptions in Lemma 6.1). The deciding factor is whether or not  $(1, 1) \in \text{App}_W$ : when  $G = \{\text{Sp}(d, 3), \text{SO}^\epsilon(d, 3)\}$  things break down.

**7.1. Finding the Special Element.** In the **FindSpecialElement** procedure, we assume that we have access to an oracle providing random elements of  $H = \langle X \rangle$ : we denote by  $\xi_H$  the time required to produce such elements. In practice, we use the built-in functions of GAP and MAGMA to produce random or pseudo-random elements (in the GAP code, we use the built-in function **PseudoRandom**, and in the MAGMA implementation, the builtin function **Random**). We require a

polynomial-time ‘test for suitability’, which takes a matrix  $g \in G$  as input and returns **TRUE** if  $g$  is a special element, and **FALSE** otherwise. Of course, computing directly the eigenvalues of an element and checking that their number is sufficiently high would work (and would ultimately not effect the analysis of the procedure’s complexity), but we wish to discard unsuitable choices as quickly as possible. The name **FindSpecialElement** is slightly inaccurate: we require our elements to be  $\text{ppd}(d, q; d')$ -elements with sufficiently many 1-dimensional eigenspaces (specifically, we ask that the  $\ell_{ij}$ -eigenspace be 1-dimensional for all  $(i, j) \in \text{App}_W$ ). Such elements form a superset of the special elements: in Section 8.1, we find lower bounds on the proportion of special elements in  $G$ , which automatically gives a lower bound on the probability that a randomly chosen element of  $H$  will have the desired properties.

In order to find a special element in the case  $G = \text{SU}(d, q)$  with  $d$  even, we do not simply search for them: instead, we search for a more abundant type of element from which a special element can be constructed. Note that here and henceforth, we consider  $\text{SU}(d, q)$  to be a subgroup of  $\text{SL}(d, q)$ , defined only when  $q$  is a square.

**Definition 7.1.** Let  $G = \text{SU}(d, q)$ , with  $d$  even, and let  $d' = d - 1$ . Then  $s \in G$  is called a *pre-special element* of  $G$  if  $o(s) = \sqrt{q}^{d'} + 1$ .

**Lemma 7.2.** Let  $G = \text{SU}(d, q)$ , with  $d$  even and  $d \geq 4$ , and let  $s$  be a pre-special element of  $G$ . Then  $s^{\sqrt{q}+1}$  is a special element.

*Proof.* This follows immediately from the definitions of special and pre-special elements: since  $\sqrt{q} + 1$  divides  $o(s)$  the order of  $s^{\sqrt{q}+1}$  is  $\frac{\sqrt{q}^{d'}+1}{\sqrt{q}+1}$ . Also, any primitive prime divisor  $r$  of  $\sqrt{q}^{d'} - 1$  must be coprime to  $\sqrt{q} + 1$ , since  $(\sqrt{q} + 1) \mid q - 1$ , and so  $r \nmid (\sqrt{q} + 1)$ : thus  $r \mid o(s^{\sqrt{q}+1})$ , and so  $s^{\sqrt{q}+1}$  is a  $\text{ppd}(d, q; d')$ -element.  $\square$

As part of our test for specialness, we require a polynomial-time test for whether an element  $s \in G$  has order divisible by a primitive prime divisor of  $q^{d'} - 1$ . Since we will know the eigenvalues of  $s$  when the time comes, it is cheaper to decide if the order of an eigenvalue is divisible by a primitive prime divisor  $r$  of  $q^{d'} - 1$ : since  $o(\lambda) \mid o(s)$  for every eigenvalue  $\lambda$  of  $s$ , if  $r \mid o(\lambda)$  then  $s$  is a  $\text{ppd}(d, q; d')$ -element.

**Lemma 7.3.** If  $(q, d') = (2, 6)$ , set  $m := 21$ . If  $(q, d') = (p, 2)$  for  $p$  a Mersenne prime, then set  $m := p - 1$ . For all other pairs  $(q, d')$  with  $q$  a prime power and  $d' > 2$ , set

$$m := \prod_{\substack{j \mid d' \\ j < d'}} \frac{d'}{j} (q^j - 1).$$

Suppose that  $\lambda \in K = \mathbb{F}_{q^{d'}}$ , and  $\lambda^m \neq 1$ . Then  $\lambda \in G$  has order divisible by a primitive prime divisor of  $q^{d'} - 1$ .

*Proof.* For an integer  $x$ , denote by  $(x)_r$  the  $r$ -part of  $x$ , that is, the largest power of  $r$  dividing  $x$ . Suppose that  $r$  is a prime divisor of  $o(s)$ , and suppose that  $e$  is the smallest integer such that  $r \mid q^e - 1$ . Suppose that  $1 \leq e < d'$  (that is,  $r$  is not a primitive prime divisor of  $q^{d'} - 1$ , and let  $(q^e - 1)_r = r^t$ . Suppose that  $r \neq 2$ : then by [18, Lemma 4.1(iii)], we have that  $(q^{d'} - 1)_r = r^t \left(\frac{d'}{e}\right)_r = (q^e - 1)_r \left(\frac{d'}{e}\right)_r$ . Thus the  $r$ -part of  $q^{d'} - 1$  divides the  $j = e$  term in the product defining  $m$ , and so  $r$

does not divide the order of  $\lambda^m$ .

Suppose that  $r = 2$ : then  $q$  is odd, since if  $q$  is even then  $r \nmid q^{d'} - 1$ . If  $d$  is even, then  $q^{d'} - 1 = (q^{d'/2} - 1)(q^{d'/2} + 1)$ , and since  $q$  is odd, we have  $q^{d'/2} \equiv 1$  modulo 4, and so  $(q^{d'/2} + 1)_2 = 2$ . Then  $(q^{d'} - 1)_2 = 2(q^{d'/2} - 1)_2$ , and so the  $j = d'/2$  term of the product defining  $m$  is divisible by the 2-part of  $o(\lambda)$ . It follows that 2 does not divide the order of  $\lambda^m$ . If  $d$  is odd, then  $(q^{d'} - 1)/(q - 1) = 1 + \dots + q^{d'-1}$  is the sum of an odd number of odd numbers, and so is odd. That is,  $(q^{d'} - 1)_2 = (q - 1)_2$ . Thus the  $j = 1$  term of the product defining  $m$  is divisible by the 2-part of  $q^{d'} - 1$ , and so 2 does not divide the order of  $\lambda^m$ .

Then since  $o(\lambda^m) \mid o(\lambda)$ , the only prime divisors of  $o(\lambda^m)$  are the primitive prime divisors of  $q^{d'} - 1$  which divide  $o(\lambda)$ , and the result follows. In the exceptional cases (when  $(q, d') = (2, 6)$  or  $(p, 2)$  for  $p$  a Mersenne prime) the result follows by a similar argument.  $\square$

**Remark 7.4.** Since the number of divisors of  $d'$  is less than  $2\sqrt{d'}$ , we have that  $m = O(q^{d'+d'(2\sqrt{d'})}) = O(q^{d^{3/2}})$ . Then by applying Lemma 7.3 to a known eigenvalue of  $s$  in  $K$ , we can decide if  $s$  is a  $\text{ppd}(d, q; d')$ -element in  $O(\rho_{q^{d'}} \log m) = O(\rho_{q^{d'}} \log(q^{d^{3/2}})) = O(\rho_{q^{d'}} d^{3/2} \log q)$  time.

Note that this task requires that we can completely factorise  $d'$ : we do not concern ourselves with the cost of non-field-operations. Since our computations take place in a field of size  $q^{d'}$ , the cost of factoring  $d'$  will be small compared to the cost of field operations.

The biggest speedup we can perform on the test for specialness is to avoid factoring the characteristic polynomial completely over  $K$  if it is unnecessary: in particular it follows from the results below about the orbits of eigenvalues over  $K$  that the characteristic polynomial of a special element has no irreducible factors over  $F$  of any degree other than  $1, 2, \frac{d'}{2}$  or  $d'$ , and in fact we know explicitly their distributions (which depend on the case). With this knowledge in our hand, we can eliminate most unsuitable candidates beforehand, and not waste our time computing the eigenvalues over  $K$ . Recall that  $\text{App}_W(s)$  is the set of pairs  $(i, j)$  such that the  $\ell_{ij}$ -eigenspace of  $s_{W_K}$  is 1-dimensional.

**Proposition 7.5.** *Algorithm 1 is a Las Vegas algorithm which returns, with probability at least  $1 - \epsilon$ , an element  $g$  of  $H$  such that the following hold:*

- (i)  $g$  is a  $\text{ppd}(d, q; d')$ -element;
- (ii) *There exists a labelling of the eigenvalues of  $g$  as  $\{\ell_{ij} \mid (i, j) \in \text{App}_W\}$ , such that the eigenspace of  $\ell_{ij}$  is 1-dimensional for all  $(i, j) \in \text{App}_W$  (see Lemma 6.2);*

and has complexity

$$O\left((\xi_H + \rho_q d^3(d^3 + \log q) + \rho_{q^{d'}} d^3 \log^2 d \log(dq)) \frac{1}{P} \log \epsilon^{-1}\right),$$

where  $P$  is the proportion of special elements in  $G$ . In particular, using the bound  $P > \frac{1}{9d^2 \log^2 q}$  (see Section 8.1 and Table 5), we have that  $\frac{2}{P} < \frac{9}{2} d^2 \log^2 q$ , and so



**Algorithm 1** FindSpecialElement

**Input:** A set  $X \subseteq \text{GL}(n, q)$ , such that  $H = \langle X \rangle$  generates a nontrivial section  $W$  of  $S^2(V)$ , represented as  $n \times n$  matrices over  $F = \mathbb{F}_q$ , and an acceptable probability of failure  $\epsilon \in (0, 1)$ .

**Output:** A  $\text{ppd}(d, q; d')$ -element of  $H$ , together with its (unlabelled) eigenvalues  $\ell_{ij}$ , separated into  $\sigma$ -orbits (where  $\sigma$  is the Frobenius automorphism  $x \mapsto x^q$ ).

**Procedure:**

- (i) Set  $T := \lceil \frac{2}{P} \log(\epsilon^{-1}) \rceil$ , where  $P$  is the lower bound for the proportion  $|S|/|G|$  given in Table 5 below.
- (ii) If more than  $T$  random elements of  $H$  have been requested, then return **FAIL**. Otherwise, choose a random element  $g \in H$ , and compute the characteristic polynomial  $c_g(t)$  of  $g$ .
- (iii) Compute the square-free factorisation of  $c_g(t)$  (see [10, Section 4.6]). If  $c_g(t)$  has a square divisor which is not a power of  $(t - 1)$ , then discard  $g$  and return to (ii).
- (iv) Compute the distinct-degree factorisation of  $c_g(t)$  (see [8, Algorithm D]), which yields the number of irreducible factors of each degree  $d', d'/2, 2, 1$ . If the degrees are not correct, then discard  $g$  and return to (i); if they are, then  $g$  has the correct number and arrangement of orbits of eigenvalues in  $W_K$ .
- (v) Compute the distinct linear factors of  $c_g(t)$  over  $K$  (using, for example, the algorithm of Beals et al. [1, Lemma 4.6]), and hence the eigenvalues of  $g$  over  $K$ . For a zero  $\beta \in K$  of one of the irreducible divisors of  $c_g(t)$  of largest degree, compute  $\beta^m$ , for  $m$  as in Lemma 7.3. If the value is 1, or if the computation of linear factors returns **FAIL**, then discard  $g$  and return to (ii).
- (vi) In the case  $G = \text{SU}(d, q)$  for  $d$  even, if  $s$  does *not* have 1 as an eigenvalue, compute the  $(q + 1)$ st power of each eigenvalue. If these powers are all distinct, then return  $g^{q+1}$  and its eigenvalues. If not, then return to (ii).
- (vii) In all other cases, return  $g$  and its eigenvalues over  $K$ .

*Algorithm 1 has complexity*

$$O\left((\xi_H + \rho_q d^3 (d^3 + \log q) + \rho_{q^{d'}} d^3 \log^2 d \log(dq)) d^2 \log^2 q \log \epsilon^{-1}\right)$$

*Proof.* It is possible that we may fail to detect the unsuitability of an element until the very last test in (vi), and so in the worst case, we must run (i)–(vi) on  $T$  matrices. Step (ii) costs  $O(\xi_H + \rho_q d^6)$ . Step (iii) costs  $O(\rho_q d^3 \log q)$  and (iv) runs faster than (iii).

We can find the distinct linear factors of the characteristic polynomial using the Las Vegas algorithm of [1] in time

$$O\left(\rho_{q^{d'}} n \log n \log(nq^d) \log \log n \log \epsilon^{-1}\right) = O\left(\rho_{q^{d'}} d^3 \log^2 d \log(dq) \log \epsilon^{-1}\right).$$

and testing whether  $\beta^m = 1$  requires time  $O(\rho_{q^{d'}} d^{3/2} \log q)$  by Remark 7.4. Thus each test has total worst-case cost

$$O\left(\rho_q (d^6 + d^3 \log q) + \rho_{q^{d'}} d^3 \log^2 d \log(dq) \log \epsilon^{-1}\right).$$

The result then follows since every special element will pass, and so  $T$  tests is sufficient to ensure that the probability of failure is at most  $\epsilon$  (note that the  $\epsilon$  introduced by the factoring algorithm is a different value, and we may have to split our error probability between the two: this is a mere technicality and we omit dealing with it for the sake of space and time).  $\square$

**7.2. Labelling the Eigenvalues  $\ell_{ij}$ .** The goal of this section is to present the family of `LabelEigenvalues` procedures which, given the eigenvalues and corresponding eigenspaces of a special element  $s \in H$  in  $W_K$ , produce a valid labelling of their orbits according to the structure given in Lemma 6.1.

**Definition 7.6.** An assignment  $(i, j) \mapsto \ell_{ij}$  is called a *valid labelling of eigenvalues* if there exists a set  $\{\ell_i \mid 1 \leq i \leq d\}$  such that, for every pair  $1 \leq i \leq j \leq d$ , we have  $\ell_{ij} = \ell_i \ell_j$ .

A valid labelling of the  $\ell_{ij}$  allows us to find eigenvectors  $f_{ij}$  for  $W_K$  satisfying the conditions of Lemma 6.8. While naive searching would suffice to perform this task ‘quickly enough’ (in the sense that this part of `Initialise` is not a bottleneck), nevertheless we employ shortcuts to speed up the process.

We proceed case by case, according to the value of  $d'$  as defined in Table 2: recall that  $d' \in \{d-2, d-1, d\}$ .

**7.2.1. The Case  $d' = d$ .** In this case, the eigenvalues of  $s$  in its action on  $W_K$  are, by Lemma 6.1,

$$\{\ell_{ij} \mid 1 \leq i \leq j \leq d\}.$$

It follows directly from the definition that for every  $i, j$ , we have  $\ell_{ii}\ell_{jj} = \ell_{ij}^2$  – that is, the  $\sigma$ -orbit  $\Omega$  containing  $\ell_{11}$  has the property that the product of any two distinct members of  $\Omega$  is the square of an eigenvalue in another orbit. Our procedure uses this property to find a suitable  $\ell_{11}$  by eliminating those orbits which do not possess the property.

We begin by storing in memory the set of squares of the eigenvalues. Then choosing at random a candidate for  $\ell_{11}$ , we test whether  $\ell_{11}^{1+q^{j-1}}$  (which is equal to  $\ell_{11}\ell_{jj}$ ) lies in this set of squares for  $2 \leq j \leq d$ . If this test fails for any  $j$ , we select another orbit and try again. Since the square root operation is very costly for large fields  $K$ , and since we do not need to know the square root of  $\ell_{11}^{1+q^{j-1}}$  explicitly – only whether or not it is one of the  $\ell_{ij}$  – the memory we use to hold this relatively small lookup table is a small price to pay for a much faster procedure.

**Remark 7.7.** (i) In step (i) of `LabelEigenvaluesSymSquare(d'=d)` (and in subsequent `LabelEigenvalues` procedures outlined below) we do not simply compute the  $\sigma$ -orbits of eigenvalues, but retain a record of the  $q$ th power of each eigenvalue. In practice this is achieved by storing each orbit as an ordered list, with each entry the  $q$ th power of its predecessor. This step requires  $O(d^2)$   $q$ th-power computations, each with a cost of  $O(\rho_{q^{d'}} \log q)$ , and so the setup of this data structure has complexity  $O(\rho_{q^{d'}} d^2 \log q)$ . Once this data structure has been set up, computation of  $q^k$ th powers of eigenvalues has zero cost (to find the  $q^k$ th power of an eigenvalue we simply move  $k$  spaces down the list), and hence computation of  $(q^k + 1)$ st powers can hence be performed with a single field operation.

**Algorithm 2** LabelEigenvaluesSymSquare( $d'=d$ )

**Input:** A special element  $s \in H$ , and the eigenvalues of  $s$  in its action on  $W_K$ , in the case that  $d' = d$ .

**Output:** A valid labelled set  $\{\ell_{ij} \mid 1 \leq i \leq j \leq d\}$  of eigenvalues, and a basis  $\mathcal{F}_W = \{f_{ij} \mid (i, j) \in \text{App}_W\} \cup \mathcal{F}'$  of  $W_K$ , satisfying the conditions in Lemma 6.8.

**Procedure:**

- (i) Compute the  $q$ th power of each eigenvalue, and sort them into ordered  $\sigma$ -orbits.
- (ii) Compute the square of each eigenvalue, and store these in a list  $\Sigma^2$ , with a record of the correspondence between eigenvalues and their squares.
- (iii) For each orbit  $\Omega$  of eigenvalues, choose an element  $\alpha \in \Omega$ . For  $2 \leq k \leq d-1$ , compute  $\alpha^{q^{k-1}+1}$ . If the result lies in  $\Sigma^2$ , find its square root and label it  $\ell_{1k}$ ; if not, then discard  $\Omega$  and choose another orbit. Once all of  $\ell_{1k}$  have been labelled, proceed to (iv).
- (iv) For  $2 \leq i < j \leq d$ , label  $\ell_{ij} = \ell_{i-1, j-1}^q$ .
- (v) For each  $(1, j) \in \text{App}_W$ , set  $f_{1j}$  to be the eigenvector of  $\ell_{1j}$  having a 1 in its first nonzero entry.
- (vi) For  $(i, j) \in \text{App}_W$  with  $i \geq 2$ , set  $f_{ij} = f_{i-1, j-1}^\sigma$ .
- (vii) If necessary, extend  $\{f_{ij} \mid (i, j) \in \text{App}_W\}$  to a basis for  $W_K$  in any way: these eigenvectors are of no consequence to us.

- (ii) In step (iii) of LabelEigenvaluesSymSquare( $d'=d$ ), the computation of square roots is free, since in step (ii) we store a correspondence between eigenvalues and their squares. This has a relatively small memory cost, and saves a considerable amount of time, since taking a square root in  $K$  has a cost of  $O(\rho_{q^{d'}} d \log q)$ .
- (iii) In practice we perform the final step, of extending the partial basis  $\{f_{ij} \mid (i, j) \in \text{App}_W\}$  to a basis for  $W_K$ , by computing a basis for the 1-eigenspace of  $s$  in  $W_K$  (or, in fact, in  $W$ , since the 1-eigenspace has a basis consisting only of  $F$ -vectors: the distinction is of little consequence).

**Proposition 7.8.** *Algorithm 2 (LabelEigenvaluesSymSquare( $d'=d$ )) returns a valid labelling  $\{\ell_{ij} \mid 1 \leq i \leq j \leq d\}$  of the eigenvalues of  $s$  on  $W_K$  together with a basis  $\mathcal{F}_W = \{f_{W,ij} \mid (i, j) \in \text{App}_W\} \cup \mathcal{F}'$  for  $W_K$  satisfying the conditions in Lemma 6.8; and has complexity*

$$O(\rho_{q^{d'}} d^4 (d^3 + \log q)),$$

where  $\rho_{q^{d'}}$  is the cost of a field operation in  $K = \mathbb{F}_{q^{d'}}$ .

*Proof.* Steps (iii)-(iv) yield a valid choice of  $\ell_{11}$ : setting  $\ell_1$  to be a square root of this value and setting  $\ell_i = \ell_1^{q^{i-1}}$  we have that  $\ell_{ij} = \ell_i \ell_j$  – that is, we have a valid labelling of the eigenvalues. Note that the orbit of the true value of  $\ell_{11}$  must be tested (since all orbits are tried), and the choice within that orbit is unimportant (for choosing another element of the orbit simply relabels the  $\ell_i$  by a cyclic permutation), and so the algorithm terminates after testing every orbit in the worst case. Since for  $(i, j) \in \text{App}_W$ ,  $f_{ij}$  is an  $\ell_{ij}$ -eigenvector, and  $\mathcal{F}_W$  satisfies the  $\sigma$ -relations in the Symmetric Square case for  $(i, j) \in \text{App}_W$  (see Definition 6.3) by the construction in step (vi),  $\mathcal{F}_W$  satisfies the conditions of Lemma 6.8.

Step (i) costs  $O(\rho_{q^{d'}} d^2 \log q)$ , by Remark 7.7(i). Steps (ii)-(iii) cost  $O(d^2)$ , since there are  $O(d^2)$  squares to take in step (ii), and in the worst case there are  $d$  orbits to try, and  $d - 1$  powers  $\alpha^{q^k+1}$  to test.

Since the  $q$ th power of every eigenvalue is known (from (i)), step (iv) costs nothing: by labelling the first element in an orbit, we implicitly label the entire orbit (see Remark 7.7(i)). Step (v) requires at most  $d$  eigenvector calculations at a cost of  $O(\rho_{q^{d'}} d^6)$  each, and (vi) involves computing a  $q$ th power of an element of  $K$   $O(d^4)$  times, each of which is  $O(\rho_{q^{d'}} \log q)$ , and so step (vi) is  $O(\rho_{q^{d'}} d^4 \log q)$ . Step (vii) costs less than (v) since we may complete it by considering the 1-eigenspace. Combining these runtimes, Algorithm 2 is  $O(\rho_{q^{d'}} (d^7 + d^4 \log q))$ .  $\square$

**7.2.2. The Case  $d' = d - 1$ .** In this case, we have that  $\ell_d = 1$ , and so the eigenvalues of  $s$  in its action on  $W_K$  are, by Lemma 6.1,

$$\{\ell_{ij} \mid 1 \leq i \leq j \leq d\} = \{1\} \cup \{\ell_{id} = \ell_i \mid 1 \leq i \leq d'\} \cup \{\ell_{ij} \mid 1 \leq i \leq j \leq d'\}.$$

We now present the algorithm `LabelEigenvaluesSymSquare(d'=d-1)`, which applies to all of these cases. We proceed similarly to the case  $d' = d$  above, but this time we identify a suitable candidate for the orbit of  $\ell_{1d} = \ell_1$  by noting that  $\ell_{1d}^{q^{k-1}+1} = \ell_{1k}$  for  $1 \leq k \leq d'$ .

---

**Algorithm 3** `LabelEigenvaluesSymSquare(d'=d-1)`

---

**Input:** A special element  $s \in H$ , and the eigenvalues of  $s$  in its action on  $W_K$ , in the case that  $d' = d - 1$ .

**Output:** A valid labelled set  $\{\ell_{ij} \mid 1 \leq i \leq j \leq d\}$  of eigenvalues, and a basis  $\mathcal{F}_W = \{f_{ij} \mid (i, j) \in \text{App}_W\} \cup \mathcal{F}'$  of  $W_K$ , satisfying the conditions in Lemma 6.8.

**Procedure:**

- (i) Compute the  $q$ th power of each eigenvalue, and sort them into ordered  $\sigma$ -orbits.
  - (ii) For each orbit  $\Omega$  of eigenvalues, and choose an element  $\alpha \in \Omega$  and label  $\ell_{1d} := \alpha$ . For  $1 \leq k \leq d - 1$ , compute  $\alpha^{q^{k-1}+1}$ . If the result is an eigenvalue, label it  $\ell_{1k}$ ; if not, then discard all labels, and choose another orbit  $\Omega$ . Once all of  $\ell_{1k}$  have been labelled, proceed to (iii).
  - (iii) For  $2 \leq i \leq d'$ , label  $\ell_{id} = \ell_{1d}^{q^{i-1}}$ ; for  $2 \leq i \leq j \leq d'$ , label  $\ell_{ij} = \ell_{i-1, j-1}^q$ .
  - (iv) For each  $(1, j) \in \text{App}_W$ , set  $f_{1j}$  to be the eigenvector of  $\ell_{1j}$  having a 1 in its first nonzero entry.
  - (v) For  $(i, j) \in \text{App}_W$  with  $i > 1$ , compute  $f_{ij}$  using the  $\sigma$ -relations in Definition 6.3.
  - (vi) If necessary, extend  $\{f_{ij} \mid (i, j) \in \text{App}_W\}$  to a basis for  $W_K$  in any way.
- 

**Proposition 7.9.** *Algorithm 3 (`LabelEigenvaluesSymSquare(d'=d-1)`) returns a valid labelling  $\{\ell_{ij} \mid 1 \leq i \leq j \leq d\}$  of the eigenvalues of  $s$  on  $W_K$  together with a basis  $\mathcal{F}_W = \{f_{ij} \mid (i, j) \in \text{App}_W\} \cup \mathcal{F}'$  for  $W_K$  satisfying the conditions in Lemma 6.8; and has complexity*

$$O(\rho_{q^{d'}} d^4 (d^3 + \log q)),$$

where  $\rho_{q^{d'}}$  is the cost of a field operation in  $K = \mathbb{F}_{q^{d'}}$ .

*Proof.* Setting  $\ell_i = \ell_{id}$  for  $1 \leq i \leq d'$ , and  $\ell_d = 1$ , we have  $\ell_{ij} = \ell_i \ell_j$  for  $1 \leq i \leq j \leq d$ , and so the labelling  $\ell_{ij}$  is valid. Since every orbit is tested, the procedure will eventually find an orbit (the true orbit of  $\ell_{1d}$ ) satisfying this condition, and so always returns a valid labelling. Since for each  $f_{ij}$  we have that  $f_{ij}$  is an  $\ell_{ij}$ -eigenvector, and by the construction of  $f_{ij}$  in (v)  $\mathcal{F}_W$  satisfies the  $\sigma$ -relations in the Symmetric Square case for all  $(i, j) \in \text{App}_W$  (see Definition 6.3), we have that  $\mathcal{F}_W$  satisfies the conditions of Lemma 6.8.

Step (i) has complexity  $O(\rho_{q^{d'}} d^2 \log q)$  (see Remark 7.7(i)), and after performing this step we can compute each power  $\lambda^{q^{k-1}+1}$  with just one field multiplication in  $K$ . Thus we are guaranteed to find a suitable  $\ell_{1d}$  after at most  $d^2$  multiplications in  $K$ , and so step (ii) has complexity  $O(\rho_{q^{d'}} d^2)$ . Step (iii) is ‘free’ since we have completed step (i) (again by Remark 7.7(i)).

Step (iv) requires at most  $d$  eigenvector calculations at a cost of  $O(\rho_{q^{d'}} d^6)$  each, and (v) involves computing a  $q$ th power of an element of  $K$   $O(d^4)$  times, each of which is  $O(\rho_{q^{d'}} \log q)$ , and so the cost of step (v) is  $O(\rho_{q^{d'}} d^4 \log q)$ . Step (vi) costs less than step (iv), since we may complete it by a computation of the 1-eigenspace. Combining these runtimes, the total cost of Algorithm 3 is  $O(\rho_{q^{d'}} (d^7 + d^4 \log q))$ .  $\square$

**7.2.3. The Case  $d' = d - 2$ .** In the case  $d' = d - 2$ , we label  $\ell_{d-1} = m_1, \ell_d = m_2$ , where  $m_i = \mu^{q^{i-1}}$ , so the eigenvalues of  $s$  in its action on  $W_K$  are, by Lemma 6.1 and since  $m_1 m_2 = \mu^{q+1} = 1$ ,

$$\{1\} \cup \{\ell_i m_j \mid 1 \leq i \leq d', 1 \leq j \leq 2\} \cup \{\ell_{ij} \mid 1 \leq i \leq j \leq d'\} \cup \{m_1^2, m_2^2\}.$$

We approach the problem by trying to identify those two  $\sigma$ -orbits of eigenvalues containing  $\ell_1 m_1, \ell_1 m_2$  respectively. Our knowledge of  $m_1^2$  makes the process of eliminating unsuitable candidates easy, since the orbit  $\Omega$  of  $\ell_1 m_1$  has the property that  $\frac{m_2}{m_1} \Omega$  is itself the orbit of  $\ell_1 m_2$ .

**Proposition 7.10.** *Algorithm 4 (`LabelEigenvaluesSymSquare(d'=d-2)`) a valid labelling  $\{\ell_{ij} \mid 1 \leq i \leq j \leq d\}$  of the eigenvalues of  $s$  on  $W_K$  together with a basis  $\mathcal{F}_W = \{f_{ij} \mid (i, j) \in \text{App}_W\} \cup \mathcal{F}'$  for  $W_K$  satisfying the conditions in Lemma 6.8; and has complexity*

$$O(\rho_{q^{d'}} d^4 (d^3 + \log q)),$$

where  $\rho_{q^{d'}}$  is the cost of a field operation in  $K$ .

*Proof.* Setting  $m_1$  as a square root of the chosen  $m_1^2$  in step (ii), and  $\ell_i = (\ell_i m_1)/m_1$  for  $1 \leq i \leq d'$ ,  $\ell_{d-1} = m_1, \ell_d = m_1^q$ , we have for all  $(i, j)$  that  $\ell_{ij} = \ell_i \ell_j$ , and this is a correct labelling of the eigenvalues, and since every orbit is tested in steps (iii)-(v), an orbit satisfying these properties is found, since the true orbit of  $\ell_1 m_1$  must eventually be tested. Since for all  $\ell_{ij}$  we chose  $f_{ij}$  to be an  $\ell_{ij}$ -eigenvector, and we construct  $f_{ij}$  in step (viii) to satisfy the  $\sigma$ -relations for all  $(i, j) \in \text{App}_W$  (see Definition 6.3), the basis  $\mathcal{F}_W$  satisfies the conditions of Lemma 6.8.

Step (i) involves  $d^2$   $q$ th-power calculations, and so costs  $O(\rho_{q^{d'}} d^2 \log q)$  (see Remark 7.7(i)). Step (ii) requires 2  $q$ th-power calculations (in the sense that we take powers bounded above by  $q$ ), and so has complexity  $O(\rho_{q^{d'}} \log q)$ . Getting from step (iii) to the successful completion of step (v), in the worst case, requires the

---

**Algorithm 4** LabelEigenvaluesSymSquare( $d'=d-2$ )

---

**Input:** A special element  $s \in H$ , and the eigenvalues of  $s$  in its action on  $W_K$ , in the case that  $d' = d - 2 \geq 6$ .

**Output:** A valid labelled set  $\{\ell_{ij} \mid 1 \leq i \leq j \leq d\}$  of eigenvalues, and a basis  $\mathcal{F}_W = \{f_{ij} \mid (i, j) \in \text{App}_W\} \cup \mathcal{F}'$  of  $W_K$ , satisfying the conditions in Lemma 6.8.

**Procedure:**

- (i) Compute the  $q$ th power of each eigenvalue, and sort them into ordered  $\sigma$ -orbits.
  - (ii) There is exactly one orbit of length 2, namely  $\{m_1^2, m_2^2\}$ : choose one eigenvalue from this orbit and label it  $m_1^2$ . Compute  $\alpha = \frac{m_2}{m_1}$  as  $(m_1^2)^{(q-1)/2}$  (recall  $q$  is odd, so  $(m_1^2)^{(q-1)/2} = m_1^{q-1} = m_2/m_1$ ).
  - (iii) For each remaining orbit  $\Omega$ , choose  $\beta \in \Omega$  and compute  $\alpha\beta$ . If this is an eigenvalue, label  $\beta = \ell_1 m_1, \alpha\beta = \ell_1 m_2$  and proceed to (iv). If not, then try another orbit  $\Omega$ .
  - (iv) For  $2 \leq i \leq d'$ , label  $\ell_i m_2 = (\ell_{i-1} m_1)^q, \ell_i m_1 = (\ell_{i-1} m_2)^q$ .
  - (v) For  $2 \leq k \leq d'$ , compute  $\ell_{1k} = (\ell_1 m_1)(\ell_k m_2)$ . If this is not an eigenvalue, return to (iii) and choose another orbit  $\Omega$ .
  - (vi) For  $(i, j) \in \text{App}_W$  with  $i \geq 2$ , label  $\ell_{ij} = \ell_{i-1, j-1}^q$ .
  - (vii) For each  $(1, j) \in \text{App}_W$ , set  $f_{1j}$  to be the eigenvector of  $\ell_{1j}$  having a 1 in the first nonzero entry.
  - (viii) For  $(i, j) \in \text{App}_W$  with  $i > 1$ , compute  $f_{ij}$  using the  $\sigma$ -relations in Definition 6.3.
  - (ix) If necessary, extend  $\{f_{ij} \mid (i, j) \in \text{App}_W\}$  to a basis for  $W_K$  in any way.
- 

testing of  $d$  orbits, and each test requires  $d$  field multiplications – note that by Remark 7.7(i), steps (iv), (vi) have zero cost – hence steps (iii)-(vi) together have complexity  $O(\rho_{q^{d'}} d^2)$ .

Step (vii) requires at most  $d$  eigenvector calculations at a cost of  $O(\rho_{q^{d'}} d^6)$  each, and (viii) involves computing a  $q$ th power of an element of  $K$   $O(d^4)$  times, each of which has complexity  $O(\rho_{q^{d'}} \log q)$ , and so step (viii) costs  $O(\rho_{q^{d'}} d^4 \log q)$ . Step (ix) costs less than step (vii), since we may complete it by computing the 1-eigenspace of  $s$ . Combining these runtimes, Algorithm 4 is  $O(\rho_{q^{d'}} (d^7 + d^4 \log q))$ .  $\square$

**7.3. Avoiding Division By Zero.** In the following steps of the algorithm there is a small chance that our procedure may attempt to divide by zero! To deal with this (very real) possibility we again use the techniques of randomised algorithms, and so we need to address two things: we must decide what to do when a division by zero is attempted, and we must bound the probability that the need will arise. Should a division by zero be attempted during one of the **FindConstants** family of procedures, we simply observe that these procedures depend upon a random selection in the group  $H$ , and the division by zero is, in fact, dependent on the random choice made. Thus it is easily fixed by choosing another random element (of course, if this continues to occur we must return **FAIL**).

If a division by zero is attempted during one of the **FindPreimage** family of procedures, we must somehow ‘inject’ randomness into proceedings: should  $g \in G$ , the

input to **FindPreimage**, cause an error, we choose a random  $h \in H$ , and compute preimages under  $\varphi$  of  $h, gh^{-1}$ . Then the preimage of  $g$  is found by computing

$$\varphi^{-1}(g) = \varphi^{-1}(gh^{-1})\varphi^{-1}(h),$$

where here we use the notation  $\varphi^{-1}(h)$  to mean a representative of the preimage: since this gives only a sign ambiguity, this is well-defined and gives the full preimage of  $g$ . We now describe precisely the conditions under which a division by zero may be attempted.

**Definition 7.11.** Let  $K = \mathbb{F}_{q^{d'}}$ , and let  $(a_{ij}) \in \text{GL}(d, K)$ . Then  $(a_{ij})$  is said to have the *divisibility property* if  $a_{ij} \neq 0$  for all  $(i, j) \in \text{App}_W$ .

**Lemma 7.12.** Let  $K = \mathbb{F}_{q^{d'}}$  for  $q$  odd, let  $(a_{ij}) \in \text{GL}(d, q^{d'})$ , and for each  $(i, j), (k, \ell) \in \text{App}_W$ , suppose that  $\kappa_{ij,kl} = \frac{c_{ij}}{c_{kl}}(a_{ik}a_{j\ell} + (1 - \delta_{ij})a_{i\ell}a_{jk})$ , for  $c_{ij}, c_{kl} \neq 0$ . Then  $(a_{ij})$  has the divisibility property if and only if, for every  $i, j, k$  with  $(i, i), (i, j), (j, k), (k, k) \in \text{App}_W$ , we have  $\kappa_{ii,jk}, \kappa_{ij,kk} \neq 0$ .

*Proof.* This follows immediately from the Basic Equations, since  $\kappa_{ii,jk} = \frac{c_{ii}}{c_{jk}}a_{ij}a_{ik}$ ,  $\kappa_{ij,kk} = 2\frac{c_{ij}}{c_{kk}}a_{ik}a_{jk}$  and since  $q$  is odd and all of the  $c_{ij}$  are nonzero.  $\square$

In [14, Lemma 4.8], Magaard, O'Brien & Seress managed to find a lower bound on the proportion of elements of an arbitrary subgroup  $G \leq \text{GL}(d, K)$  having the divisibility property in the Symmetric Square Case for  $G \cong \text{SL}(d, q)$ : however, their argument depends entirely on the large order of  $\text{SL}(d, q)$ , and hence cannot be applied to the other classical groups. We require a conjecture that a similar result holds:

**Conjecture 7.13.** Let  $s \in G$  be a special element, and let  $\{f_i\}$  be a basis of eigenvectors for  $s_{V_K}$  as described in Lemma 3.6. Let  $g \in G$  be a random element of  $G$ , and let  $(a_{ij})$  be the matrix of  $g$  with respect to the basis  $\mathcal{F}_V := \{f_i \mid 1 \leq i \leq d\}$  of  $V_K$ . Then

- (i) For each  $i, j$  we have  $P(a_{ij} = 0) < \frac{4}{q^d}$ ; and
- (ii)  $P(a_{ij} \neq 0, \forall i, j) > \frac{5}{8}$ .

When  $G = \text{GL}(d, q)$ , this is precisely the statement of Lemma 4.8 in [14] (albeit with slightly different notation). To computationally test Conjecture 7.13, we construct a random conjugate of  $G$  in  $\text{GL}(d, K)$ , and choose a random sample of matrices from this random conjugate (in practice, we produce a random element  $h \in \text{GL}(d, K)$ , choose random elements  $\{g_i\}$  from a standard copy of  $G$ , and test their conjugates  $\{g_i^h\}$ ). We tested all groups  $\text{SL}(d, q), \text{SU}(d, q), \text{Sp}(d, q), \text{SO}^\epsilon(d, q)$  for all relevant  $d \leq 12, q \leq 13$ : we tested 10 random conjugates of the group in  $\text{GL}(d, K)$ , and chose from each conjugate 100 random elements. We found *no* case of a matrix failing to possess the divisibility property. Of course, it is easy to construct matrices which fail to possess the divisibility property: for example in the Symmetric Square case, most ‘nice’ matrices, including the identity matrix, do not have the property. However, the sheer size of  $\text{GL}(d, K)$  means that a random conjugate of  $G$  is unlikely to contain many ‘nice’ matrices.

**7.4. Finding the Constants  $c_{ij}$ .** Having found, using the appropriate variant of **LabelEigenvalues** in Section 7.2 above, a basis  $\mathcal{F}_W$  satisfying the conditions of Lemma 6.8, we know (by the conclusions of this Lemma and Corollary 6.9) that

there exist bases  $\mathcal{F}_V, \mathcal{F}_V^-$  for  $V_L$ , and sets  $\mathcal{C} = \{c_{ij} \mid (i, j) \in \text{App}_W\}, \mathcal{C}^- = \{c_{ij}^- \mid (i, j) \in \text{App}_W\} \subset L$ , such that the action of  $g \in G$  on  $\mathcal{F}_V$  (or  $\mathcal{F}_V^-$ ) can be calculated from the action on  $\mathcal{F}_W$ , so long as we know the values of certain  $c_{ij}$  (or  $c_{ij}^-$ ). This section is dedicated to the computation of these required constants.

Recall from Corollary 6.9 that, for every  $(i, j), (k, \ell) \in \text{App}_W$ , the *Basic Equations in the Symmetric Square Case* hold:

$$(9) \quad \kappa_{ij, k\ell} = \frac{c_{ij}}{c_{k\ell}} (a_{ik}a_{j\ell} + (1 - \delta_{ij})a_{i\ell}a_{jk}) = \frac{c_{ij}^-}{c_{k\ell}^-} (a_{ik}^-a_{j\ell}^- + (1 - \delta_{ij})a_{i\ell}^-a_{jk}^-).$$

where  $a_{ij} = g_{f_i f_j}, a_{ij}^- = g_{f_i^- f_j^-}, \kappa_{ij, k\ell} = g_{f_{ij} f_{k\ell}}$ , and  $\delta_{ij} = 1$  when  $i = j$  and 0 otherwise. The first of these equations is the key to both the process of finding  $c_{ij}$  (or  $c_{ij}^-$ ), and later, finding the matrix  $(a_{ij}) = (g_{f_i f_j})$  for an arbitrary  $g \in G$ . However, in the course of our procedures, information is lost in the case that both sides of the equation are zero: this is addressed in Section 7.3: recall from Definition 7.11 that we say a matrix  $(a_{ij}) \in \text{GL}(d, K)$  has the *divisibility property* if  $a_{ij} \neq 0$  for all  $i, j$ .

**Remark 7.14.** Throughout this section and the next, we make frequent reference to Lemma 6.2, which states (in short) that, with a few exceptional cases, we have  $\{(1, j) \mid 1 \leq j \leq d, j \neq d'/2 + 1\} \subset \text{App}_W$ . We prove several results in this section which depend upon membership in  $\text{App}_W$ , and so we do not technically require Lemma 6.2 until we ‘use’ the results to produce the Algorithms `FindConstantsSymSquare` and `FindPreimageSymSquare`. However, the reader should keep in mind that  $(1, d'/2 + 1)$  is the only possible exception to the general rule that ‘ $(1, j)$  is always in  $\text{App}_W$ ’.

Moreover, it is always true that  $(i, j) \in \text{App}_W$  whenever  $(i - 1, j - 1) \in \text{App}_W$ .

**7.4.1. Relations Between the Values  $\kappa_{ij, k\ell}, c_{ij}, a_{ij}$ .** In this section we derive certain relations between the constants  $\kappa_{ij, k\ell}, c_{ij}$ , and  $a_{ij}$ , which are obtained through manipulations of (9) along with the assumption that  $(a_{ij})$  has the divisibility property. Note that while all of these relations apply to the ‘negative’ versions of the  $a_{ij}, c_{ij}$ , we have no need for them.

**Lemma 7.15.** *Suppose that  $(1, 1), (i, j) \in \text{App}_W$ . Suppose that  $(a_{ij})$  has the divisibility property as in Definition 7.11. If  $i = j$ , then  $c_{ii} = 1$ , and if  $i < j$  then*

$$c_{ij}^2 = \frac{\kappa_{ij, jj}^2}{4\kappa_{jj, jj}\kappa_{ii, jj}}.$$

*Proof.* If  $i = j$  the result follows immediately from Corollary 6.9. Suppose now that  $i < j$ . Then by (9), noting that the  $c_{ij}$  are, by definition, never zero, and since  $\kappa_{ij, jj}, \kappa_{jj, jj} \neq 0$  since  $g$  has the divisibility property (by Lemma 7.12), we have

$$\frac{\kappa_{ij, jj}^2}{\kappa_{jj, jj}\kappa_{ii, jj}} = \frac{(\frac{c_{ij}}{c_{jj}}(2a_{ij}a_{jj}))^2}{\frac{c_{ij}}{c_{jj}}(a_{jj}a_{jj})\frac{c_{ii}}{c_{jj}}(a_{ij}a_{ij})} = 4c_{ij}^2,$$

and the result follows. Note that since  $q$  is odd, division by 4 is well-defined.  $\square$

**Lemma 7.16.** *Suppose that  $(1, 1) \in \text{App}_W$ . Then the following hold for all pairwise distinct integers  $i, j, \ell$  such that  $(i, j), (j, \ell) \in \text{App}_W$ , when  $(a_{ij})$  has the divisibility property as in Definition 7.11:*



- (i)  $\kappa_{ii,ii} = a_{ii}^2$ ;
- (ii)  $c_{ij} = \frac{a_{ii}a_{ij}}{\kappa_{ii,ij}}$ ;
- (iii) Define

$$(iii)_{i,j,\ell} := \frac{\kappa_{ii,ij}\kappa_{ij,jj}}{2\kappa_{jj,jj}\kappa_{ii,jj}} \left( \kappa_{ij,j\ell} - \frac{\kappa_{ij,jj}\kappa_{jj,j\ell}}{2\kappa_{jj,jj}} \right).$$

$$\text{Then } \frac{c_{ij}}{c_{j\ell}} a_{i\ell} a_{ii} = (iii)_{i,j,\ell}.$$

*Proof.* Part (i) follows on setting  $i = j = k = \ell$  in (9). For (ii), applying (9) with pairs  $(i, i), (i, j)$ , we have

$$\kappa_{ii,ij} = \frac{c_{ii}}{c_{ij}} (a_{ii}a_{ij}),$$

and the result follows since  $c_{ii} = 1$ , by Lemma 7.15.

For (iii), note first that applying (9), we have

$$\begin{aligned} \frac{\kappa_{ii,ij}\kappa_{ij,jj}}{2\kappa_{jj,jj}\kappa_{ii,jj}} &= \frac{(\frac{c_{ii}}{c_{ij}} a_{ii}a_{ij})(\frac{c_{ij}}{c_{jj}} 2a_{ij}a_{jj})}{2(a_{jj}^2)(\frac{c_{ii}}{c_{jj}} a_{ij}^2)} \\ &= a_{ii}a_{jj}^{-1}. \end{aligned}$$

Secondly, again applying (9),

$$\begin{aligned} \kappa_{ij,j\ell} - \frac{\kappa_{ij,jj}\kappa_{jj,j\ell}}{2\kappa_{jj,jj}} &= \frac{c_{ij}}{c_{j\ell}} (a_{ij}a_{j\ell} + a_{i\ell}a_{jj}) - \frac{(\frac{c_{ij}}{c_{jj}} 2a_{ij}a_{jj})(\frac{c_{jj}}{c_{j\ell}} a_{jj}a_{j\ell})}{2a_{jj}^2} \\ &= \frac{c_{ij}}{c_{j\ell}} (a_{ij}a_{j\ell} + a_{i\ell}a_{jj}) - \frac{c_{ij}}{c_{j\ell}} a_{ij}a_{j\ell} \\ &= \frac{c_{ij}}{c_{j\ell}} a_{i\ell}a_{jj}. \end{aligned}$$

Multiplying the two gives the result. □

We now use Lemma 7.16 to give a result which allows us to isolate the  $a_{ij}$  from the  $c_{ij}$  (we will use this to extract the  $c_{ij}$  first, and once they are known it will be relatively easy to find the  $a_{ij}$ ):

**Lemma 7.17.** *Let  $(iii)_{i,j,k}$  be defined as in Lemma 7.16(iii), let  $k > 1$  be odd, and set  $j = \frac{k+1}{2}$ . Then if  $(1,1), (1,j), (1,k), (j,k) \in \text{App}_W$ , and if  $(a_{ij})$  satisfies the divisibility property as in Definition 7.11, we have*

$$a_{1k}a_{11} = (iii)_{1,j,k} \left( \frac{\kappa_{1j,jj}^2}{4\kappa_{jj,jj}\kappa_{11,jj}} \right)^{\frac{q^j-1-1}{2}}.$$

*Proof.* By Lemma 7.16(iii), we have

$$(iii)_{1,j,k} = \frac{c_{1j}}{c_{jk}} a_{1k}a_{11}.$$

Now  $c_{jk} = c_{1j}^{q^j-1}$ , and hence  $\frac{c_{1j}}{c_{jk}} = (c_{1j}^2)^{\frac{1-q^j-1}{2}}$ . The result then follows by Lemma 7.15. □

It may seem that the result of Lemma 7.17 is sufficient to determine the  $a_{ij}$  for very many  $(i, j)$  without any care for the values of the  $c_{ij}$ . However, for simplicity, and since things become increasingly complex when there are issues with  $(i, j) \notin \text{App}_W$ , we prefer to calculate the  $c_{ij}$  in any case: it is better to deal with any potential difficulties in the preprocessing procedure **Initialise** rather than in the procedure **FindImage**, which may be run many times.

**Lemma 7.18.** *Let  $(iii)_{i,j,k}$  be defined as in Lemma 7.16(iii), let  $k > 1$  be odd, and set  $j = \frac{k+1}{2}$ . If  $(a_{ij})$  has the divisibility property as in Definition 7.11, and  $(1, 1), (1, j), (1, k), (j, k) \in \text{App}_W$ , then we have*

$$c_{1k} = \frac{(iii)_{1,j,k}}{\kappa_{11,1k}} \left( \frac{\kappa_{1j,jj}^2}{4\kappa_{jj,jj}\kappa_{11,jj}} \right)^{\frac{q^{j-1}-1}{2}}.$$

*Proof.* The result follows by applying Lemmas 7.16(ii) and 7.17 to  $c_{1k}$ . □

We now find analogous results to Lemmas 7.17 and 7.18 for even  $k$ .

**Lemma 7.19.** *Suppose that  $(1, 1), (1, 2) \in \text{App}_W$ , and suppose that  $(a_{ij})$  satisfies the divisibility property as in Definition 7.11. Let  $c'_{12}$  be a square root of*

$$\frac{\kappa_{12,22}^2}{4\kappa_{22,22}\kappa_{11,22}},$$

*and let  $y = \frac{c_{12}}{c'_{12}}$ . Then  $y \in \{\pm 1\}$ , and  $c'_{12} \in K$ . Moreover, for any even  $k > 2$ , set  $j = k/2$ . Then if  $(1, j), (1, k), (j, k-1) \in \text{App}_W$ , we have*

$$a_{1k}a_{11} = \left( (iii)_{1,2,k} \frac{(c_{1,k-1})^q}{c'_{12}} \right) y.$$

*Proof.* By Lemma 7.15, we have

$$c_{12}^2 = \frac{\kappa_{12,22}^2}{4\kappa_{22,22}\kappa_{11,22}},$$

and so since the square roots of the right hand side are  $\pm c_{12}$ , both square roots lie in  $K$ . Then labelling either of these  $c'_{12}$ , we have  $c_{12} = \pm c'_{12}$ , and so  $y = \pm 1$ .

For each  $j \leq d'/2$  with  $(1, j), (1, k), (j, k-1) \in \text{App}_W$ , set  $k = 2j$ . By Lemma 7.16(iii),

$$\frac{c_{12}}{c_{2k}} a_{1k}a_{11} = (iii)_{1,2,k},$$

and since  $c_{2k} = c_{1,k-1}^q$  we have

$$a_{1k}a_{11} = (iii)_{1,2,k} \frac{(c_{1,k-1})^q}{c_{12}} = \left( (iii)_{1,2,k} \frac{(c_{1,k-1})^q}{c'_{12}} \right) y$$

as required. □

**Lemma 7.20.** *Let  $k > 2$  be even and suppose that  $(1, 1), (1, j), (1, k), (2, k) \in \text{App}_W$ , and  $(a_{ij})$  has the divisibility property as in Definition 7.11. Let  $c'_{12}, y$  be defined as in Lemma 7.19 above, and define*

$$c'_{1k} = \frac{(iii)_{1,2,k}}{\kappa_{11,1k}} \frac{(c_{1,k-1})^q}{c'_{12}}.$$

*Then  $c_{1k} = c'_{1k}y$ .*

*Proof.* Using Lemmas 7.16(ii) and 7.19, we have

$$c_{1k} = \frac{1}{\kappa_{11,1k}} a_{11} a_{1k} = \frac{1}{\kappa_{11,1k}} \left( (iii)_{1,2,k} \frac{c_{1,k-1}^q}{c'_{12}} \right) y,$$

and the result follows.  $\square$

The following result proves that if we ‘incorrectly guessed’ the value of  $c_{12}$  (that is, if  $y = -1$ ), then we will find instead the values  $c_{ij}^-$ , and so without loss of generality we may assume that  $y = 1$ .

**Lemma 7.21.** *Let  $\mathcal{C} = \{c_{ij} \mid (i, j) \in \text{App}_W\}$ ,  $\mathcal{C}^- = \{c_{ij}^- \mid (i, j) \in \text{App}_W\}$  be as defined in Corollary 6.9. Let  $y = \pm 1$ , and define  $\mathcal{C}' := \{c'_{ij} \mid (i, j) \in \text{App}_W\}$  as follows. For  $1 \leq j \leq d'$  with  $(1, j) \in \text{App}_W$ , let*

$$c'_{1j} = \begin{cases} c_{1j} & \text{if } j \text{ is odd; and} \\ c_{1j}y & \text{if } j \text{ is even;} \end{cases}$$

*and for  $2 \leq i \leq j \leq d'$  with  $(i, j) \in \text{App}_W$ , set  $c'_{ij} = (c'_{i-1,j-1})^q$ . For  $(i, j) \in \text{App}_W$  with  $j > d'$ , set  $c'_{ij} = c_{ij}$ .*

*Then for all  $(i, j) \in \text{App}_W$ ,  $1 \leq i \leq j \leq d'$ , we have that*

$$c'_{ij} = \begin{cases} c_{ij}y & \text{if } 1 \leq i \leq j \leq d' \text{ and } j-i \text{ is odd; and} \\ c_{ij} & \text{otherwise.} \end{cases}$$

*In particular, we have*

$$\mathcal{C}' = \begin{cases} \mathcal{C} & \text{if } y = 1; \text{ and} \\ \mathcal{C}^- & \text{if } y = -1. \end{cases}$$

*Proof.* If  $i = 1$ , then the result follows immediately from the definition of  $c'_{ij}$ . We now suppose that  $i > 1$  and proceed by induction. If  $j - i$  is odd, we have that

$$c'_{ij} = (c'_{i-1,j-1})^q = (c_{i-1,j-1})^q = c_{ij}.$$

If  $j - i$  is even then

$$c'_{ij} = (c'_{i-1,j-1})^q = (c_{i-1,j-1}y)^q = c_{ij}y,$$

since  $y^q = y$ .

The second assertion follows trivially when  $y = 1$ , and when  $y = -1$  we have that the definition of  $c_{ij}^- \in \mathcal{C}^-$  matches exactly the definition of  $c'_{ij} \in \mathcal{C}'$  when  $y = -1$ .  $\square$

**Proposition 7.22.** *Assume that Conjecture 7.13 holds. Then if  $G \notin \{\text{Sp}(d, 3), \text{SO}^\epsilon(d, 3)\}$ , then Algorithm 5 returns correct values  $c_{ij} = c_{ij}^\pm$  for  $1 \leq i \leq j \leq d'$ , or FAIL; and is a Las Vegas algorithm with complexity*

$$O((\xi_H + \rho_{q^{d'}} d(d^5 + \log q)) \log \epsilon^{-1}),$$

*where  $\xi_H$  is the cost of choosing random elements from  $H$ , and  $\rho_{q^{d'}}$  is the cost of a field operation in  $K$ .*

---

**Algorithm 5** FindConstantsSymSquare
 

---

**Input:** A basis  $\mathcal{F}_W = \{f_{ij} \mid (i, j) \in \text{App}_W\} \cup \mathcal{F}'$  of  $W_K$ , satisfying the conditions in Lemma 6.8, and an acceptable probability of failure  $\epsilon \in (0, 1)$ .

**Output:** One of the sets  $\{c_{ij} \mid 1 \leq i \leq j \leq d'\}$ ,  $\{c_{ij}^- \mid 1 \leq i \leq j \leq d'\}$  as described in Corollary 6.9; or FAIL.

**Procedure:**

- (i) Choose a random element  $g \in G$ , and find the matrix  $(\kappa_{ij,kl})$  of  $g$  with respect to the basis  $\mathcal{F}_W$ . If at any time during the rest of the procedure a division by zero is attempted, choose another random element and begin again, until  $T$  selections have been made, where  $T = \lceil 4 \log \epsilon^{-1} \rceil$ . If the steps below cannot be completed on any of these  $T$  random elements then return FAIL.
- (ii) Set  $c_{11} = 1$ , and for  $2 \leq j < (d' + 1)/2$ , set  $k = 2j - 1$ , and compute

$$c_{1k} = \frac{(iii)_{1,j,k}}{\kappa_{11,1k}} \left( \frac{\kappa_{1j,jj}^2}{4\kappa_{jj,jj}\kappa_{11,jj}} \right)^{\frac{q^j-1-1}{2}},$$

where  $(iii)_{1,j,k}$  is as in Lemma 7.16(iii). This provides  $c_{1k}$  for all  $(1, k) \in \text{App}_W$  with  $k$  odd.

- (iii) Compute  $c_{12}$  as one of the square roots of

$$\frac{\kappa_{1222}^2}{4\kappa_{2222}\kappa_{1122}}.$$

- (iv) For  $2 \leq j \leq d'/2$ , set  $k = 2j$ . If  $(1, k), (2, k) \in \text{App}_W$ , then compute

$$c_{1k} = \frac{(iii)_{1,2,k}}{\kappa_{11,1k}} \frac{(c_{1,k-1})^q}{c_{12}}.$$

- (v) If there exists  $k$  such that  $(1, k) \in \text{App}_W$  and we have not yet computed  $c_{1k}$ , then  $d', d'/2$  are even and we compute

$$c_{1k} = (iii)_{13k} \frac{(c_{1,k-2})^{q^2}}{c_{13}\kappa_{11,1k}}.$$

- (vi) For  $(i, j) \in \text{App}_W$  with  $2 \leq i \leq j \leq d$ , compute  $c_{ij} = c_{i-1,j-1}^q$ .
- 

*Proof.* Subject to  $(a_{ij})$  having the divisibility property, the correctness of the values  $c_{ij}$  follows from Lemmas 7.18, 7.20, 7.21, and 6.2, noting that we may return the set  $\{c_{ij}^-\}$  in place of  $\{c_{ij}\}$ .

For each randomly selected  $g$ , we compute the matrix  $(\kappa_{ij,kl})$ : this requires matrix conjugation: conjugating by a matrix is equivalent to one inversion operation and two multiplications, for a total cost of  $O(\rho_{q^{d'}} n^3) = O(\rho_{q^{d'}} d^6)$ .

The computation of  $(iii)_{1jk}$  requires a constant number of field operations in  $K$ , and so has cost  $O(\rho_{q^{d'}})$ . Step (ii)'s most expensive operation is the computation of a power of order  $O(q^d)$ , and so its cost is  $O(\rho_{q^{d'}} \log q^d) = O(\rho_{q^{d'}} d \log q)$ . Step (iii) requires the computation of a square root in  $K$ , which has cost  $O(\rho_{q^{d'}} d \log q)$ . Steps (iv)-(vi) require only the computation of  $q$ th powers, and so have complexity less than step (ii). Thus the procedure costs  $O(\rho_{q^{d'}} (d^6 + d \log q))$  if  $(a_{ij})$  has the

divisibility property.

Assuming Conjecture 7.13 holds, we have that the probability that  $(a_{ij})$  has the divisibility property is at least  $1/2$ , and so setting  $T = \lceil 4 \log \epsilon^{-1} \rceil$ , the procedure returns **FAIL** with probability less than  $\epsilon$ , and has complexity  $O(T(\xi_H + \rho_{q^{d'}}(d^6 + d \log q))) = O((\xi_H + \rho_{q^{d'}} d^5 (d + \log q)) \log \epsilon^{-1})$ .  $\square$

## 8. PROBABILITY AND PROPORTIONS

The effectiveness of any algorithm which chooses random elements is dependent upon probability: namely, the probability that a randomly chosen element has the properties we need. In our case there are two issues at hand: the probability that a randomly chosen element has the required eigenstructure, and later that randomly chosen element do not have zeroes in places that we don't want.

**8.1. Counting Special Elements.** In this Section we determine, using the Quokka Theory of Niemeyer and Praeger, lower bounds for the proportions of Special Elements in Classical Groups. We provide only a very brief summary of Quokka Theory here: for more see [13, 19].

Quokka sets are subsets  $Q$  of a finite group  $G$  of Lie Type whose proportion in  $G$  can be found by determining certain proportions in maximal tori in  $G$  and in the Weyl group of  $G$  (respectively, an abelian group and a permutation group – both much simpler to deal with). Recall that each element  $g \in G$  has a unique Jordan decomposition  $g = su$ , where  $s \in G$  is semisimple,  $u \in G$  is unipotent and  $su = us$  (with  $s$  and  $u$  called the *semisimple part* and  $u$  the *unipotent part* of  $g$  respectively [2, p. 11]).

A nonempty subset  $Q$  of  $G = \mathrm{GL}(n, q)$  is a *quokka set* if the following two conditions hold:

- (i) if  $g \in G$  has Jordan decomposition  $g = su$  with semisimple part  $s$  and unipotent part  $u$ , then  $g \in Q$  if and only if  $s \in Q$ ;
- (ii)  $Q$  is a union of  $G$ -conjugacy classes.

By [4, Lemma XX], the characteristic polynomial of the semisimple part  $s$  of  $g$  is the same as the characteristic polynomial of  $g$ : thus all properties of the eigenvalues of a group element are preserved in this ‘transition’ to  $s$ . It follows that:

**Lemma 8.1.** *Let  $S$  be the set of Special Elements of a finite group of Lie Type  $G$  as in Definition 3.3. Then  $S$  is a Quokka set.*

Suppose that  $\overline{\mathbb{F}}_q$  is the algebraic closure of  $\mathbb{F}_q$ , with  $F$  the Frobenius morphism (so that the fixed points of  $F$  in  $\overline{\mathbb{F}}_q$  are precisely  $\mathbb{F}_q$ ). Then as outlined in [13, Section 3], choose a maximal torus  $T_0$  of  $\mathrm{GL}(n, \overline{\mathbb{F}}_q)$  so that  $W = N_{\hat{G}}(T_0)/T_0$  is the corresponding Weyl group (isomorphic to a subgroup of  $S_d$ ).

A subgroup  $H$  of the connected reductive algebraic group  $\mathrm{GL}(n, \overline{\mathbb{F}}_q)$  is said to be  $F$ -stable if  $F(H) = H$ , and for each such subgroup  $H$ , we write  $H^F = H \cap \mathrm{GL}(n, \mathbb{F}_q)$ . We define an equivalence relation on  $W$  as follows: elements  $w, w' \in W$  are  $F$ -conjugate if there exists  $x \in W$  such that  $w' = x^{-1}wx^F$ . The equivalence classes

of this relation on  $W$  are called *F-conjugacy classes* [2, p. 84]. The  $\mathrm{GL}(n, \mathbb{F}_q)$ -conjugacy classes of  $F$ -stable maximal tori are in one-to-one correspondence with the  $F$ -conjugacy classes of the Weyl group  $W$ . The explicit correspondence is given in [2, Proposition 3.3.3].

Let  $\mathcal{C}$  be the set of  $F$ -conjugacy classes in  $W$  and, for each  $C \in \mathcal{C}$ , let  $T_C$  be a representative element of the family of  $F$ -stable maximal tori corresponding to  $C$ . The following theorem is a direct consequence of [19, Theorem 1.3].

**Theorem 8.2.** *Suppose that  $Q \subseteq G = \mathrm{GL}(n, q)$  is a quokka set. Then*

$$(10) \quad \frac{|Q|}{|G|} = \sum_{C \in \mathcal{C}} \frac{|C|}{|W|} \frac{|T_C^F \cap Q|}{|T_C^F|}.$$

where  $W$  is the Weyl group of  $G$ ,  $\mathcal{C}$  is the set of conjugacy classes of  $F$ -stable maximal tori in  $G$ , and  $T_C$  is a representative torus in the conjugacy class  $C$ .

**Theorem 8.3.** *Let  $G^F$  be as in the 5th column of Table 2, let  $d$  be the natural dimension of  $G^F$ , and let  $S$  be the set of special elements of  $G$ , as defined in Definition 3.3 (see Table 2 for reference). Then the proportion  $|S|/|G^F|$  is bounded below by the corresponding value in the final column of Table 2.*

In all cases, the proof is similar to the proof of [19, Theorem 1.9], in which Niemeyer & Praeger use this theory to determine the proportion of  $\mathrm{ppd}(d; q; d')$ -elements. In particular, the arguments used there for finding the proportion  $\frac{|C|}{|W|}$  are nearly identical: the Weyl Group and proportion are as listed in Table 5. Thus we summarise the proof and give the important values in Table 5: for a very detailed proof in all cases, see [3, Chapter 6]. The maximal torus corresponding to the  $F$ -conjugacy class of  $W$  is given in the 7th column of Table 5, and is exactly as in the proof of [19, Theorem 1.9]: the only difference in our case is the extra conditions we impose on the order of a special element: this difference manifests in the proportion  $|S \cap T_C|/|T_C|$ : for this we need the following Lemma.

**Lemma 8.4.** *Let  $a$  be a positive integer, let  $G = \mathbb{Z}_a$ , and let  $X$  be the set of elements of  $G$  of order  $a$ . Then  $|X| = \varphi(a) > \frac{a}{3 \log a}$ , where  $\varphi$  is Euler's Totient Function, which counts the number of positive integers strictly less than  $a$  which are coprime to  $a$ .*

*Proof.* Let  $t$  be a divisor of  $a$ . The proportion of elements of  $\mathbb{Z}_a$  having order exactly  $t$  is  $\varphi(t)$ , and the second inequality (which we have simplified from  $\varphi(a) > \left(\frac{\log 2}{2}\right) \left(\frac{a}{\log a}\right)$  since  $\log 2 > \frac{2}{3}$ ) can be found in [15, I.1.5] (citing [6]).  $\square$

Thus in every case, we apply Lemma 8.4 to bound below the proportion of elements of the torus  $T_C$  contained in  $S$  (that is, having the required order as in Table 2), to bound below the value  $|S \cap T_C|/|T_C|$ , with the results given in the 9th column of Table 5 (in the case  $d' = d - 2$ , we must apply Lemma 8.4 twice: once to each cyclic component). We obtain a lower bound for  $|S|/|G|$  (10th column) by combining this with the proportion  $|C|/|W|$  (8th column) found in [19, 3].

## 9. IMPLEMENTATIONS

The original (unofficially released) implementation of this algorithm was in GAP and at the time of writing has been made public at the first author's website, or by direct contact. It is likely to be implemented in a more official way in the

$\mathrm{SL}(10, q) \leq \mathrm{GL}(55, q)$				
	Black Box		New	
$q$	Init	Preimage	Init	Preimage
4	2.402	0.13354	0.07025	0.00815
9	33.727	2.13191	1.33375	0.171835
37	232.847	8.57023	1.95	0.0902475
$\mathrm{Sp}(10, q) \leq \mathrm{GL}(55, q)$				
	Black Box		New	
$q$	Init	Preimage	Init	Preimage
5	3.338	0.22542	0.429	0.042745
9	30.904	1.60463	1.174	0.0689925
37	150.806	5.46581	1.478	0.1212525

TABLE 3. Comparison of runtimes (in seconds) between Black Box and specialised algorithms in MAGMA.

$q$	4		5		8	
SL( $d, q$ )						
$d$	Init	Preimage	Init	Preimage	Init	Preimage
10	0.1405	1.63	0.9205	7.839	0.398	1.607
14	1.5365	4.493	6.872	95.527	5	7.4645
20	17.9245	19.227	89.1155	922.863	17.8075	24.2035
Sp( $d, q$ )						
$d$	Init	Preimage	Init	Preimage	Init	Preimage
10	0.117	0.011465	0.67475	0.071	0.503	0.0197725
14	1.84475	0.0457875	6.279	0.941465	3.8845	0.0523775
20	18.2205	0.183105	123.12775	9.5988575	20.0345	0.2331425
SU( $d, q$ ) – $d$ even						
$d$	Init	Preimage	Init	Preimage	Init	Preimage
10	0.823	0.061035	2.05525	0.12909	1.3805	0.0757375
14	5.9865	0.0974225	23.18175	2.5565	4.368	0.0771025
20	25.1825	0.2919175	315.3325	28.06579	47.56475	0.556885
SU( $d, q$ ) – $d$ odd						
$d$	Init	Preimage	Init	Preimage	Init	Preimage
9	0.542	0.0047575	3.15	0.009985	0.9905	0.007565
13	1.68875	0.0157175	22.5265	0.30116	3.7635	0.023165
19	45.5795	0.1873175	227.84325	10.75861	76.5225	0.22316
$q$	5		7		9	
SO <sup>−</sup> ( $d, q$ )						
$d$	Init	Preimage	Init	Preimage	Init	Preimage
10	0.706	0.06244	0.75275	0.0753875	1.02575	0.0678225
14	7.176	0.945755	7.96775	1.265245	21.99625	2.5359525
20	126.275	9.5132925	135.2685	12.0210075	177.7475	15.30327
SO <sup>+</sup> ( $d, q$ )						
$d$	Init	Preimage	Init	Preimage	Init	Preimage
10	0.10925	0.0102175	0.90875	0.0780775	1.2285	0.077415
14	7.141	0.83285	0.513	0.8535975	14.1765	2.0481375
20	96.54125	9.5089875	112.348	9.8805575	150.4045	13.3346925
SO <sup>0</sup> ( $d, q$ )						
$d$	Init	Preimage	Init	Preimage	Init	Preimage
9	0.113	0.01439	0.35875	0.034555	0.57325	0.0407175
13	2.258	0.21146	2.453	0.2374325	4.18075	0.3691775
19	61.875	8.86234	55.31025	7.1629025	108.90825	10.0354275

TABLE 4. Average runtimes (in seconds) for various groups (in MAGMA).



Case	$d$	$G$	$F$	$G^F$	$W$	Structure of Torus $T_C$	$\frac{ C }{ W }$	lb for $\frac{ S \cap T_C }{ T_C }$	lb for $\frac{ S }{ G }$	Condition
$A_r$	$r + 1$	$\mathrm{GL}(d, \overline{\mathbb{F}}_q)$	$\sigma_q$	$\mathrm{GL}(r + 1, q)$	$S_{r+1}$	$\mathbb{Z}_{\frac{q^d-1}{q-1} \gcd(d, q-1)}$	$\frac{1}{d}$	$\frac{1}{3d \log q}$	$\frac{1}{3d^2 \log q}$	
${}^2A_r$	$r + 1$	$\mathrm{SU}(d, \overline{\mathbb{F}}_q)$	$\sigma_q(-T)$	$\mathrm{SU}(r + 1, q)$	$S_{r+1}$	$\mathbb{Z}_{\frac{q^{d+1}-1}{q+1} \gcd(d, q+1)}$	$\frac{1}{d}$	$\frac{1}{4d \log q}$	$\frac{1}{4d^2 \log q}$	$d$ odd
						$\mathbb{Z}_{q^{d-1}+1}$	$\frac{1}{d-1}$	$\frac{1}{3d \log q}$	$\frac{1}{3d^2 \log q}$	$d$ even
$B_r$	$2r + 1$	$\mathrm{SO}(d, \overline{\mathbb{F}}_q)$	$\sigma_q$	$\mathrm{SO}(2r + 1, q)$	$S_2 \wr S_r$	$\mathbb{Z}_{q^{(d-1)/2}+1}$	$\frac{1}{d-1}$	$\frac{1}{3d \log q}$	$\frac{1}{3d^2 \log q}$	
$C_r$	$2r$	$\mathrm{Sp}(d, \overline{\mathbb{F}}_q)$	$\sigma_q$	$\mathrm{Sp}(2r, q)$	$S_2 \wr S_r$	$\mathbb{Z}_{q^{d/2}+1}$	$\frac{1}{d}$	$\frac{1}{3d \log q}$	$\frac{1}{3d^2 \log q}$	
$D_r$	$2r$	$\mathrm{SO}^+(d, \overline{\mathbb{F}}_q)$	$\sigma_q$	$\mathrm{SO}^+(2r, q)$	$(S_2 \wr S_r) \cap A_{2r}$	$\mathbb{Z}_{q^{(d-2)/2}+1} \times \mathbb{Z}_{q+1}$	$\frac{1}{d-2}$	$\frac{1}{9d \log^2 q}$	$\frac{1}{9d^2 \log^2 q}$	
${}^2D_r$	$2r$	$\mathrm{SO}^-(d, \overline{\mathbb{F}}_q)$	$\sigma_q(-T)$	$\mathrm{SO}^-(2r, q)$	$(S_2 \wr S_r) \cap A_{2r}$	$\mathbb{Z}_{q^{d/2}+1}$	$\frac{2}{d}$	$\frac{1}{3d \log q}$	$\frac{2}{3d^2 \log q}$	

TABLE 5. Weyl Group and Torus Structure for Counting Special Elements in Classical Groups

future. A MAGMA implementation of this and other functions (namely, similar algorithms for all absolutely irreducible modules of degree at most  $d^2$ ) is also in development, and the Symmetric Square case is complete. We perform tests using the implementation in MAGMA, comparing the runtimes (in seconds) in the Linear case against MAGMA's algorithm `RecogniseSL`, and in the Symplectic case against MAGMA's `RecogniseSpOdd`. Both are implementations of the Kantor-Seress Black Box algorithm [9]. Note that while in the Linear case, the Magaard-O'Brien-Seress algorithm [14] is implemented in GAP, this is essentially identical to our algorithm, and so we compare against the Black Box algorithm to illustrate the effectiveness of our methods. In practice, our implementation is slightly more efficient than the existing implementation, and both are considerably faster than the Black Box (of course, the Black Box methods have a much wider scope).

The MAGMA implementation was produced in July 2013, with the help and hospitality of the University of Auckland (in particular, Professor Eamonn O'Brien).

We provide this comparison (see Table 3) in the Linear and Symplectic cases, and the runtime gains in all cases are comparable. Table 4 gives sample runtimes for all cases for various values of  $d$  and  $q$ . The stated runtimes are averaged over several runs of `Initialise` and several hundred runs of `FindPreimage`. All times are given in seconds.

## REFERENCES

- [1] Robert Beals, Charles R Leedham-Green, Alice C Niemeyer, Cheryl E Praeger, and Ákos Seress. Constructive recognition of finite alternating and symmetric groups acting as matrix groups on their natural permutation modules. *Journal of Algebra*, 292(1):4–46, 2005.
- [2] Roger W. Carter. *Finite groups of Lie type: Conjugacy classes and complex characters*. Wiley, 1993.
- [3] Brian Corr. *Estimation and Computation with Matrices Over Finite Fields*. PhD thesis, PhD thesis, University of Western Australia, 2013.
- [4] Brian P. Corr, Tomasz Popiel, and Cheryl E. Praeger. Nilpotent-independent sets and counting in matrix algebras. 2014. In Preparation.
- [5] B. Hartley and T. O. Hawkes. *Rings, modules and linear algebra*. Chapman & Hall, London, 1980.
- [6] H Hatalová and T Šalát. Remarks on two results in the elementary theory of numbers. *Acta Fac. Rerum Natur. Univ. Comenian. Math*, 20:113–117, 1970.
- [7] Derek F Holt, Charles R Leedham-Green, EA O'Brien, and Sarah Rees. Testing matrix groups for primitivity. *Journal of Algebra*, 184(3):795–817, 1996.
- [8] Erich Kaltofen and Victor Shoup. Subquadratic-time factoring of polynomials over finite fields. *Mathematics of Computation of the American Mathematical Society*, 67(223):1179–1197, 1998.
- [9] William M Kantor and Ákos Seress. *Black box classical groups*. Number 708 in Memoirs of the American Mathematical Society. American Mathematical Society, 2001.
- [10] Donald E Knuth. Volume 2: Seminumerical algorithms. *The Art of Computer Programming*, page 192, 1997.
- [11] Charles R Leedham-Green. The computational matrix group project. *Groups and computation III*, 8:229–247, 2001.
- [12] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.
- [13] Frank Lübeck, Alice C Niemeyer, and Cheryl E Praeger. Finding involutions in finite lie type groups of odd characteristic. *Journal of Algebra*, 321(11):3397–3417, 2009.

- [14] Kay Magaard, EA O'Brien, and Ákos Seress. Recognition of small dimensional representations of general linear groups. *J. Aust. Math. Soc.*, 85(2):229–250, 2008.
- [15] DS Mitrinovic, J Sándor, and B Crstici. *Handbook of Number Theory, Mathematics and Its Applications 351*. Kluwer Academic Publishers, 1996.
- [16] Peter M Neumann and Cheryl E Praeger. A recognition algorithm for special linear groups. *Proc. London Math. Soc.*, 65(432):555–603, 1992.
- [17] Max Neunhöffer and Ákos Seress. A data structure for a uniform approach to computations with finite groups. In *Proceedings of the 2006 international symposium on Symbolic and algebraic computation*, pages 254–261. ACM, 2006.
- [18] Alice C Niemeyer, Tomasz Popiel, and Cheryl E Praeger. Abundant  $p$ -singular elements in finite classical groups. *arXiv preprint arXiv:1205.1454*, 2012.
- [19] Alice C Niemeyer and Cheryl E Praeger. Estimating proportions of elements in finite groups of Lie type. *Journal of Algebra*, 324(1):122–145, 2010.
- [20] EA O'Brien. Towards effective algorithms for linear groups. In *Finite Geometries, Groups, and Computation: Proceedings of the Conference "Finite Geometries, Groups, and Computation", Pingree Park, Colorado, USA, September 4-9, 2004*, page 163. Walter de Gruyter, 2006.

BRIAN P. CORR,  
 CENTRE FOR MATHEMATICS OF SYMMETRY AND COMPUTATION,  
 SCHOOL OF MATHEMATICS AND STATISTICS,  
 THE UNIVERSITY OF WESTERN AUSTRALIA, CRAWLEY, WA 6009, AUSTRALIA  
*Current address:* Departamento de Matemática,  
 Instituto de Ciências Exatas,  
 Universidade Federal de Minas Gerais,  
 Av. Antônio Carlos, 6627, 31270-901,  
 Belo Horizonte, MG, Brazil  
*E-mail address:* `brian.p.corr@gmail.com`